INFORMATIEBEVEILIGING MAGAZINE

DOSSIER 1

Apeldoorn- IT congres 2025

DOSSIER 2

Richtlijnen, normen en zekerheid

JAARGANG 26 - 2026 - EDITIE 1

INFORMATIEBEVEILIGING
MAGAZINE

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

Terugkijkend op de toekomst.

Chris de Vries

Het is een tijd van terugkijken alsook een verwachtingsvolle blik naar de toekomst, meestentijds geassocieerd met een positief gevoel, maar of dit voor 2026 geldt?

Wij zagen de terugkeer van Trump. En met hem handels- en fysieke oorlogen, tarieven-chantage en narcistisch gedrag, niet alleen de president kenmerkende, maar ook 'bij de zijnen' ('cum suis', lees dus de multimiljardairs en hun 'big (tech)' bedrijven).

Dat verwoordend in de "National Security Strategy of the USA" dat onverbloemd stelt de democratieën van Europa naar Amerikaans model om te vormen. Als stimulant (1) voor dié rechtse partijen die de Europese Unie (ons centrale zenuwstelsel) wensen te vernietigen, gebaseerd op nationalisme en de Amerikaanse (wereld)visie.
Trump claimt de westelijke hemisfeer (van Noord- tot Zuidpool) en brengt de olievelden van Venezuela onder zijn zeggenschap, een (militair) lot dat Groenland, wellicht het Caribisch gebied en andere ook te wachten staat.

Dit belooft veel slechts voor 2026.
Europa zal moeten vechten voor lijfsbehoud; nu nog altijd technologisch afhankelijk van de 'big tech', voor militaire bescherming van Amerikaanse, twijfelachtige ondersteuning (onwil), voor olie en gas van Rusland en voor goedkope ((cyber)technologische) producten en/of productiecapaciteit van China's marktdumping.

Harde keuzes moeten volgen. Zware investeringen in (cyber)technologie; productiecapaciteit terughalen naar Europa; grondstoffen veiligstellen (samenwerking met Afrika!?) en de logistieke lijnen meer in eigen hand nemen. High Tech kennis (2) moet in Europa blijven en beschermd worden voor de massale cyberdiefstallen/aanvallen.

Diepte-investeringen dus in onafhankelijke Europese (cyber) hard- & software innovaties, verhoging van onze (cybersecurity) defensie en een veel hoger bewustzijn van cybersecurity urgentie. In dit nummer werkt onze sector InformatieBeveiliging nijver aan bescherming van onze kennis. Van digitale hygiëne naar gecontroleerde innovatie, NIS2 en pragmatische implementatie van ISO27001 bij het MKB tot een Apeldoorns IT-event (congres 2025). Zie ook het artikel over het Functioneel Beheer dat uitgaat van een 'mindset' en dus niet van een trucje.

Al deze initiatieven voor een krachtig Nederland en daarmee bijdragende aan de Europese sterkte. Een inhoud dat juist in deze interessante tijd (een Chinese vloek!) van betekenis is. Ik wens alle lezers deze 'mindset' toe alsook een voorspoedig en impulsrijk 2026.

Chris

(1) Bewust gekozen voor een parallelle interpretatie naar psycho-analytische drugs die het centrale zenuwstelsel beïnvloeden/aantasten.
(2) Zie het dossier: "Security tech transfer", InformatieBeveiliging Magazine, jaargang 25, 2025 – editie 3.

IN DIT NUMMER

Auteurs: Corrie Jonkers, Wim Florijn en Aron Noordhoek zijn allen werkzaam bij het Data Science Team van het Kadaster. Zij zijn bereikbaar via e-mail: datascience@kadaster.nl

Gecontroleerde innovatie

de weg naar een veilige en generiek inzetbare Kadaster-chatbot

De digitale overheid krijgt steeds meer vorm en is tegenwoordig zichtbaar aanwezig, zeker sinds de razendsnelle opmars van generatieve AI. Ook bij het Kadaster wordt volop onderzocht hoe AI kan worden ingezet, bijvoorbeeld als digitale assistent. Zo wordt gekeken hoe AI complexe en versnipperde informatie toegankelijk en begrijpelijk kan maken, uiteraard met oog voor privacy en veiligheid en altijd met tussenkomst van een persoon.

Hiervoor is een interne, generieke en flexibel inzetbare chatbot-applicatie ontwikkeld die medewerkers snel en eenvoudig toegang biedt tot relevante kennis. Dit artikel laat zien hoe deze chatbot tot stand kwam, welke randvoorwaarden en ontwerpkeuzes centraal staan en hoe de architectuur van de chatbot inzet op veiligheid, transparantie en datasoevereiniteit.

Het dilemma van AI binnen de publieke sector

Generatieve AI brengt zowel kansen als uitdagingen aan het licht: enerzijds is er de roep om innovatie, anderzijds de zorg over datasoevereiniteit en ethiek. Large Language Models (LLM's) zijn een krachtig middel om kennis toegankelijk en begrijpelijk te maken. Dit leidde bij het Kadaster tot een snelle toename van pilots, direct gedreven door een behoefte vanuit de organisatie. Medewerkers zoeken bijvoorbeeld naar manieren om efficiënter te werken en een chatbot, die in natuurlijke taal laagdrempelig toegang biedt tot kennisbanken en complexe handleidingen, kan hierin een uitstekende oplossing bieden.

Toch brengen deze technologische vooruitgangen ook risico's met zich mee. Denk aan het risico op datalekken of het genereren van onjuiste informatie. Dit kan leiden tot ongewenste gevolgen, zeker als mensen vertrouwen op deze technologie voor het nemen van beslissingen. Daarom verschuift de vraag van puur technisch experimenteren naar een bredere uitdaging: hoe zorg je ervoor dat LLM's op een veilige en verantwoorde manier kunnen worden ingezet binnen heldere grenzen?

Dit leidde tot de ontwikkeling van chatbot 'Kaatje'. Binnen de architectuur van Kaatje is datatoegang strikt geregeld via authenticatie en functioneren de AI-modellen volledig binnen een gecontroleerde, afgeschermde omgeving. Deze opzet borgt zowel veiligheid, herbruikbaarheid als brede inzetbaarheid, waardoor de organisatie op verantwoorde wijze kan profiteren van de kracht van AI.

Onze opdracht: veilige, transparante en generiek toepasbare AI

We zijn gestart met een brede verkenning naar de mogelijke opzet van Kaatje. Het doel was om te onderzoeken hoe we een chatbot-architectuur konden ontwikkelen die flexibel genoeg is om uiteenlopende vraagstukken binnen het Kadaster te ondersteunen, zonder voor elk nieuw gebruiksscenario een aparte applicatie te hoeven bouwen. Tijdens deze verkenning zijn vier kernvereisten geformuleerd waaraan de oplossing moest voldoen.

Ten eerste is aanpasbaarheid essentieel. Een generieke oplossing heeft weinig waarde als deze niet mee kan bewegen met uiteenlopende behoeften. De chatbot moet eenvoudig worden afgestemd op verschillende gebruikers en usecases. Van een landmeter die documentatie over zijn meettoestel zoekt, tot de servicedesk-medewerker die wil weten hoe hij een printer koppelt. Dit vereist een architectuur waarin databronnen, koppelingen en integraties via tool-calling (agentic AI) en conversatiestijlen modulair kunnen worden in- of uitgeschakeld, zonder code te herschrijven.

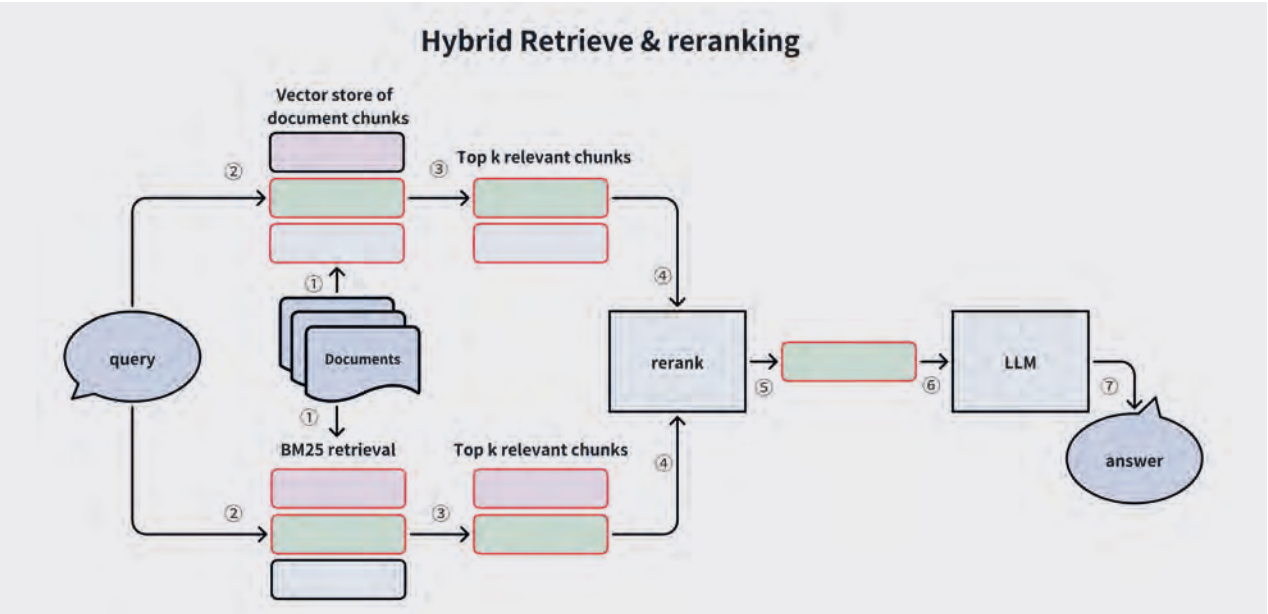
De architectuur kent twee vereiste pijlers: realtime informatie-opvraging en betrouwbare databeveiliging. We kiezen bewust voor een opzet waarbij het model antwoorden genereert op basis van actuele externe bronnen, in plaats van op kennis die tijdens een trainingsfase in het model is ingebakken. Dit elimineert de noodzaak om continu te hertrainen; het up-to-date houden van de bronnen volstaat. Deze aanpak vormt eveneens direct de basis voor de vereiste beveiliging. Doordat de kennis strikt gescheiden blijft van het taalmodel, kunnen we via authenticatie en autorisatie exact afdwingen wie toegang heeft tot welke informatie. De chatbot raadpleegt hierdoor uitsluitend bronnen waarvoor de ingelogde gebruiker specifiek rechten heeft, waarmee gevoelige data veilig en gesegmenteerd blijft per rol.

Tot slot draait de vierde kernvereiste: betrouwbaarheid, om volledig transparante herleidbaarheid. Dit betekent dat iedere uitkomst direct toetsbaar moet zijn. Binnen deze architectuur is afgedwongen dat elk antwoord gepaard gaat met expliciete verwijzingen naar de gebruikte bronnen. Dit vermindert het risico op hallucinaties en stelt de gebruiker in staat om de juistheid direct te valideren.

Implementatieopties: onze keuze voor een zelfontwikkelde oplossing

Bij de vertaling van deze missie naar een technische oplossing vormde de klassieke 'koop/maakbeslissing' het vertrekpunt. De markt voor AI-platformen ontwikkelt zich weliswaar razendsnel, maar voor het Kadaster wegen specifieke eisen rondom complexiteit en databeveiliging zwaar. Daarnaast wordt gekeken naar ongewenste afhankelijkheid van specifieke 'big tech' ecosystemen ('vendor lock-in'), waarbij we nadenken over hoe we volledige controle over de dataverwerking borgen. Begin 2025 zijn drie mogelijke routes verkend.

De eerste route, Copilot Studio, biedt een laagdrempelige 'no-code' oplossing. Het grote voordeel hiervan is de snelheid: prototyping en integratie binnen het Microsoft-ecosysteem zijn eenvoudig. Maar Copilot Studio leunt sterk op vooraf gedefinieerde dialogen, wat onvoldoende flexibiliteit biedt voor een chatbot die open, complexe vragen moet beantwoorden. Bovendien ontbreekt de generieke basis om uiteenlopende vraagstukken vanuit één centrale applicatie te bedienen.
De tweede route, Azure AI Foundry, biedt via een 'low-code' aanpak aanzienlijk meer controle. Met tools zoals Prompt Flow en integraties met Azure AI Search ontstaat er meer grip op de modellen en de evaluatie-



Figuur 1: Schematische weergave van het hybride zoekproces met reranker.

keten. Echter verkeren veel componenten nog in preview-status, waren sterk regio- of Microsoft-afhankelijk en boden niet de gewenste transparantie. De retrieval-opties binnen Foundry schoten tekort en een belangrijk punt dat mist is de flexibiliteit om bronselectie en autorisatie volgens onze eigen eisen in te richten. Dit betekent dat er te weinig mogelijkheden zijn om de instellingen zodanig aan te passen dat de kwaliteit van de opgehaalde bronnen optimaal kan worden gegarandeerd.

De derde route, en uiteindelijke keuze, is een eigen implementatie op basis van open-source frameworks en diverse taalmodellen. Deze wordt gehost via AI Foundry binnen onze eigen Azure-omgeving. Deze route verschuift de verantwoordelijkheid naar de eigen organisatie, maar biedt in ruil daarvoor volledige soevereiniteit over de code, datastructuren en integratielagen. Met deze aanpak kunnen authenticatie, fijnmazige autorisatie voor datatoegang en tooling, en specifieke retrieval-strategieën (zoals bucket-gebaseerde RAG) exact volgens de gewenste eisen worden ontworpen. Daarnaast maakt het de chatbot toekomstbestendig: de architectuur is voorbereid op een eventuele overstap naar andere taalmodellen, inclusief open-source varianten die volledig on-premise draaien. Cloudplatforms fungeren in deze opzet niet langer als allesbepalende ecosystemen, maar primair als modulaire leveranciers van hosting en rekenkracht.

Het RAG-principe: realtime ophalen en injecteren van relevante data

De kern van Kaatje wordt gevormd door een geavanceerde **R**etrieval **A**ugmented **G**eneration (RAG) architectuur. Het doel hiervan is simpel maar krachtig: domeinkennis scheiden van het taalmodel. Het taalmodel (de LLM) fungeert als een taalvaardige verwerker, terwijl de feitelijke kennis wordt aangeleverd vanuit een up-to-date database.

Het proces start met het inladen van data uit verschillende bronnen, zoals handleidingen, (web)content en instructies (Pdf's, video's). Via scraping en geavanceerde parse- en opschoontechnieken wordt deze ruwe data omgezet naar Markdown (1). Markdown is gekozen om opmaak, structuur (tabellen, koppen, lijsten) en headerinformatie te behouden, wat essentieel is voor het begrip en de chunking door het taalmodel. Door tekst te splitsen op Markdown-koppen en de metadata per fragment mee te geven, blijft de context van elke paragraaf behouden, ook als deze losstaat van het originele document.

De retrieval-laag van Kaatje, het mechanisme dat de juiste informatie zoekt bij een (op basis van het gesprek herschreven) gebruikersvraag, maakt gebruik van een hybride aanpak. Enerzijds worden 'embeddings' ingezet: wiskundige vectorrepresentaties van tekst die conceptuele gelijkenis aangeven (semantisch zoeken). Anderzijds wordt BM25 (2) gebruikt, een klassieke techniek voor het zoeken op trefwoorden (syntactisch zoeken). Deze combinatie is essentieel, omdat gebruikers vragen stellen die variëren van conceptueel ("hoe zit het met mijn

vereffeningssoftware?") tot specifieke termen als applicatienamen ("move3"). Alle data wordt hiervoor opgeslagen in een open-source database (PostgreSQL met pgvector). De resultaten van deze hybride zoekslag worden tot slot verder aangescherpt door een 'reranker'. Dit compacte taalmodel beoordeelt de gevonden resultaten opnieuw op relevantie ten opzichte van de vraag, om zo de precisie maximaal te verhogen.

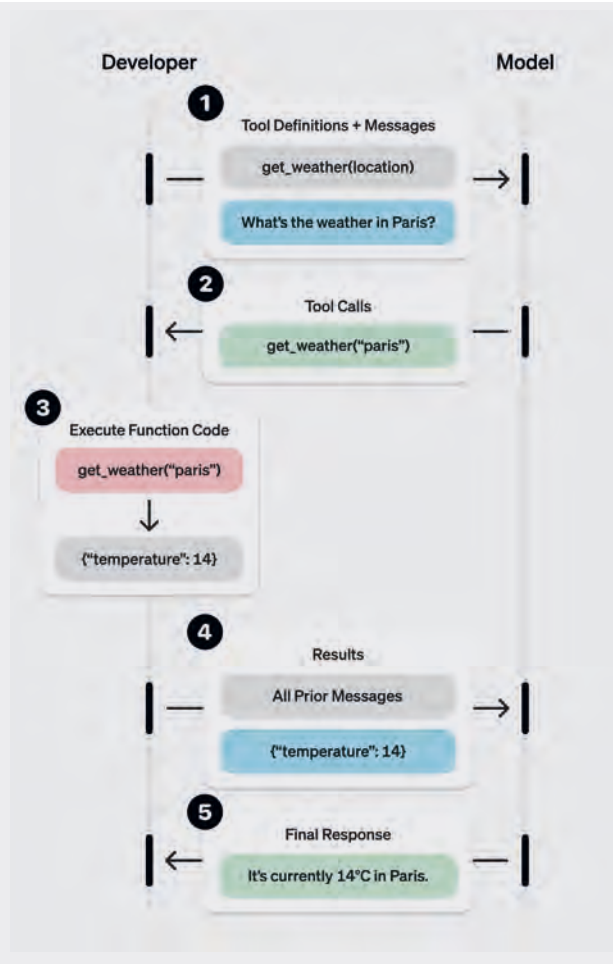
Elke chunk, een deel van een document, is gekoppeld aan het brondocument, dat op zijn beurt onderdeel is van een zogenaamde bucket: een groep documenten. De autorisatieregels bepalen welke gebruiker toegang heeft tot welke bucket. Wanneer een gebruiker een vraag stelt, wordt de zoekopdracht in de database fysiek beperkt tot alleen die rijen, die overeenkomen met zijn of haar permissies. Daardoor is het technisch onmogelijk dat bijvoorbeeld documenten van team A ongewenst worden gevonden door een medewerker van team B, ongeacht hoe slim de prompt is geformuleerd.

Agentic AI: acties uitvoeren naast het raadplegen van tekstbronnen

Kaatje beweegt eveneens voorbij de traditionele vraag-antwoordmachine richting 'Agentic AI'. Dit betekent dat het taalmodel niet beperkt is tot het verwerken van tekstinformatie, die door het RAG-systeem is geïnjecteerd, maar ook in staat is om tools te gebruiken voor het ophalen van data of het verrichten van handelingen. Dit mechanisme staat bekend als function- of tool-calling. Wij maken hiervoor gebruik van het **M**odel **C**ontext **P**rotocol (MCP) (3), een standaard die het mogelijk maakt om in de toekomst eenvoudig diverse nieuwe verbindingen in Kaatje te integreren.

Het mooie hiervan is dat het taalmodel de intentie van de gebruiker herkent en direct een gespecialiseerde functie aanroept. De PDOK-Agent (4) binnen Kaatje geeft dit principe goed weer. In dit experiment is getoetst hoe complexe databevragingen via API's volledig door de chatbot kunnen worden afgehandeld. Wanneer een gebruiker vraagt naar data over een specifiek perceel, schakelt Kaatje zelfstandig een tweede agent in. Deze voert vervolgens autonoom de benodigde stappen uit: van het omzetten van een adres naar coördinaten en het selecteren van de juiste dataset binnen PDOK, tot het daadwerkelijk uitvoeren van de query. Zo worden complexere processen toegankelijk(er) voor gebruikers, terwijl het proces transparant en controleerbaar blijft.

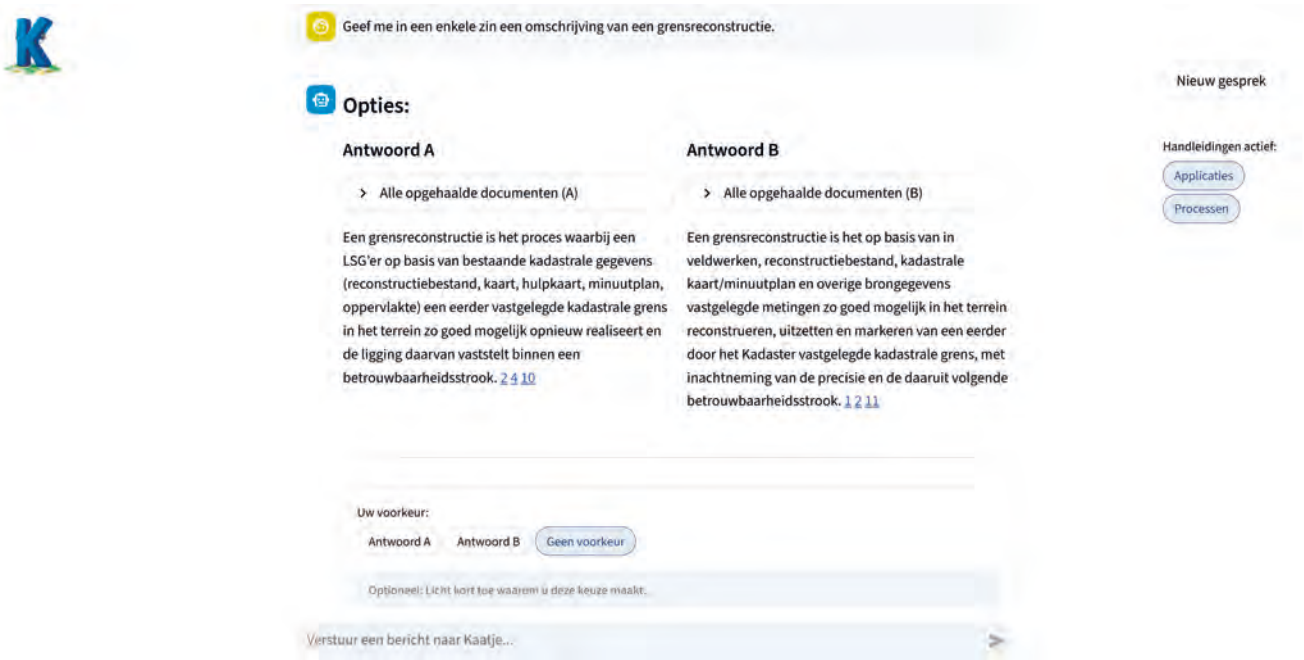
Het belangrijkste aspect hier is transparantie en afscherming. De LLM ziet nooit de volledige database, enkel de gestructureerde output van de API-aanroep. Verder ziet de gebruiker in het antwoord niet alleen de samenvatting, maar ook de onderliggende aanroep die is gedaan. De gebruiker kan hierdoor verifiëren dat de juiste parameters zijn gebruikt, en de data valideren. Ook hier geldt een strikt autorisatiemodel: een gebruiker kan alleen de tools activeren waar hij via ons centrale Identity en Access Management (IAM) systeem rechten voor heeft. Kaatje opereert dus nooit buiten het mandaat van de menselijke gebruiker.



Figuur 2: Weergave van de Agentic AI tool-calling lifecycle, gestandaardiseerd door MCP.

Kwaliteitsborging: geautomatiseerde validatie

Het ontwikkelen van een AI-systeem is slechts de eerste stap, garanderen dat het veilig en correct functioneert, is een tweede. Om subjectiviteit uit het beoordelingsproces te elimineren, is ervaring opgedaan met zowel geautomatiseerde als gebruiker-gebaseerde kwaliteitscontroles. Deze inzichten hebben geleid tot drie fundamentele pijlers.
De eerste pijler betreft geautomatiseerde validatie volgens het principe 'LLM-as-a-judge'. Hierbij evalueert een krachtig, extern taalmodel de prestaties van Kaatje. De focus ligt daarbij op 'waarheidsgetrouwheid' (is het antwoord volledig herleidbaar tot de bron?) en 'relevantie' (sluit het antwoord aan op de gestelde vraag?). Met behulp van het Ragas-



Figuur 3: Een voorbeeld van hoe de A/B-test eruitziet. De gebruiker kiest vervolgens een optie, waarna het gesprek verder gaat met het gekozen bericht.

framework (5) kunnen duizenden interacties automatisch gescoord worden op meetwaarden zoals semantische nauwkeurigheid en contextuele precisie. Dit maakt het mogelijk om de impact van technische wijzigingen, zoals een aanpassing in de 'chunking'-strategie of een nieuw 'embedding'-model, objectief te kwantificeren.

De tweede pijler omvat configuratietesten. Hierbij worden uiteenlopende taalmodellen (zoals GPT-5.2 instant versus redenatie) en systeeminstellingen zoals de hoeveelheid meegegeven broncontext, via A/B-tests met elkaar vergeleken. Dit levert kwantitatieve inzichten op in de balans tussen kosten, snelheid en kwaliteit. Op basis van deze data kan objectief worden onderbouwd of de inzet van zwaardere, kostbare modellen daadwerkelijk noodzakelijk is of dat voor specifieke usecases een efficiënter model volstaat.

De derde en belangrijkste pijler is de menselijke maat: gebruikersfeedback. Een feedbackdialoog in de interface stelt gebruikers in staat om antwoorden te beoordelen. Bij deze feedback worden logs uit het retrieval- en generatieproces opgeslagen om Kaatje effectief te kunnen verbeteren. Zo kunnen foutpatronen direct herleid worden tot een specifieke bron, een falende tool of een niet-passende modelinstelling.

Conclusie: een geslaagde technische verkenning

De verkenning van het Kadaster Data Science Team met Kaatje kan worden beschouwd als een geslaagde technische proef, die waardevolle inzichten biedt. Met de afronding van deze verkenning is een generiek fundament gelegd dat aantoont dat innovatie en regelgeving elkaar kunnen versterken en tot een beter product leiden, mits de architectuur zorgvuldig is ontworpen. Momenteel wordt Kaatje binnen het Kadaster in de praktijk getoetst door twee gebruikersgroepen. De eerste reacties zijn erg positief: gebruikers rapporteren aanzienlijke tijdsbesparing door de efficiëntere informatievoorziening. Parallel hieraan wordt onderzocht hoe Kaatje organisatiebreed kan worden uitgerold, zodat meer afdelingen en processen kunnen profiteren van deze veilige en flexibele AI-oplossing.

Referenties

(1) Voor een toelichting zie: https://www.markdown.nl/
(2) Zie voor toelichting: https://www.geeksforgeeks.org/nlp/what-is-bm25-best-matching-25-algorithm/ en https://en.wikipedia.org/wiki/Okapi_BM25
(3) Zie voor toelichting: https://github.com/modelcontextprotocol en https://en.wikipedia.org/wiki/Model_Context_Protocol
(4) PDOK = Publieke Dienstverlening Op de Kaart
(5) RAGAS = Retrieval Augmented Generation ASsessments

COLUMN LEX

25 jaar verschuiving in securitymanagement

Steeds vaker zie ik mezelf gebogen over gedetailleerde Excel-sheets, waar ik vroeger verdween in architecturen en ontwerpen. Is securitymanagement van technische vernuftigheid verworden tot administratieve vastlegging?

In 2001 zag cybersecurity er overzichtelijk uit. De vijand was zichtbaar, het speelveld was afgebakend en succes werd gemeten aan de hand van uitkomsten: gehackt worden was gefaald hebben. Vijfentwintig jaar later is dat wereldbeeld fundamenteel veranderd. Cybersecurity is formeler en complexer geworden – en tegelijk van existentieel belang. Vier grote verschuivingen tekenen die ontwikkeling scherp af.

Van uitkomstgedreven naar compliancegedreven

Aanvankelijk draaide security om resultaat. Er waren nauwelijks management standaarden. Nu is ISO 27001 dé standaard der standaarden. Firewalls werden geplaatst, virusscanners geïnstalleerd en zolang de systemen draaiden, voelde men zich veilig. Cyberincidenten waren uitzonderingen, geen dagelijkse realiteit zoals nu. Als je geluk had vroegen bestuurders: "Zijn we veilig?", meestal was het securitybewustzijn nog niet zover.

Die vraag voelt inmiddels bijna naïef. Cyberincidenten zijn onvermijdelijk; de echte vraag is of je "in control" bent. Wet- en regelgeving zoals AVG, NIS2, DORA en andere normen hebben de focus verschoven naar aantoonbaarheid. Niet alleen wat je doet, maar vooral hoe je kunt bewijzen dat je het structureel doet, telt. Dashboards, audits en maturity-modellen zijn minstens zo belangrijk geworden als technische maatregelen.

Van netwerk-centrisch naar identiteitscentrisch

In 2001 was het netwerk de kern van beveiliging. Binnen was veilig, buiten was gevaarlijk. VPN's, DMZ's en perimeter-firewalls vormden de verdedigingslinie. Wie eenmaal binnen was, kreeg impliciet vertrouwen.

Die wereld bestaat niet meer. Cloud, SaaS, thuiswerken en mobiele apparaten hebben de netwerkgrenzen weggevaagd. Nu is identiteit de nieuwe perimeter. Wie je bent, wat je mag, waar je vandaan komt en onder welke omstandigheden je toegang vraagt: dat bepaalt alles. De principes van Zero Trust (het minst betekenisvolle buzzword dat we gekend hebben) zijn nu een noodzakelijke realiteit. Identity & Access Management (IAM) is uitgegroeid tot een strategisch kernproces, naast de klassieke netwerkbeveiliging, als je tenminste nog een eigen netwerk hebt.

Van amateuristisch naar volwaardige AI – aan beide kanten

De aanvallers van 2001 waren vaak individuen of kleine groepen, met beperkte middelen en veel handwerk. Maatregelen waren simpel en overzichtelijk, al was het wel vaak een zoektocht naar de juiste techniek. Verdediging kon het tempo van de aanvaller bijhouden.

Vandaag is phishing gepersonaliseerd, malware past zich realtime aan en aanvallen worden geautomatiseerd op schaal. AI is volledig geïntegreerd in zowel aanval als verdediging. Security Operations Centers (ook iets nieuws) zouden simpelweg verdrinken zonder machine learning en automatisering. De strijd is daarmee veranderd in een AI-tegen-AI dynamiek, waarin automatisering een cruciale rol speelt. Wie niet meekomt, wordt gehackt.

Van "onze security" naar security in de hele keten

Misschien wel de meest ingrijpende verschuiving: security houdt niet meer op bij de eigen voordeur. In 2001 was er nauwelijks cloud en waren leveranciers een IT-detail. Nu zijn cloudproviders, softwareleveranciers en logistieke partners een strategisch risico.

Grote incidenten laten keer op keer zien dat zwakke schakels in de keten vaak de ingang vormen. Securitymanagement betekent daarom ketenmanagement: due diligence, contractuele eisen, continue monitoring en gezamenlijke responsplannen. Vertrouwen is vervangen door contractueel geregeld gecontroleerd wantrouwen.

Cybersecuritymanagement is in 25 jaar volwassen geworden, maar ook zwaarder, formeler en complexer. Waar het ooit een technisch probleem was, is het nu een bestuursvraagstuk met de bijbehorende administratieve lasten. Niet alleen "hoe beschermen we onze systemen?", maar "hoe organiseren we een uitstraling van vertrouwen in een digitale wereld?" Ja, het is deels een boekhoudprobleem geworden, maar achter elke cel schuilt nog de oude, vertrouwde realiteit: mensen, processen en techniek die samen het verschil maken.

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

Auteur: Daniël E. Brouwer is spreker alsook auteur van 9 boeken en 'Lean six sigma master black belt'. Hij is een expert op het gebied van Functioneel Beheer en is oprichter van VFB – Slimmer functioneel beheer. Hij is bereikbaar via: daniel.brouwer@vfb.nl

Functioneel Beheer is geen trucje, maar een mindset!

Functioneel Beheer wordt nog vaak gezien als een operationele functie. Iemand die meldingen afhandelt, testjes uitvoert en zorgt dat applicaties 'gewoon werken'. En natuurlijk: dát hoort erbij. Maar wie denkt dat Functioneel Beheer daar stopt, ziet iets belangrijks over het hoofd.

Een goede functioneel beheerder is geen uitvoerder, maar een denker, doener én verbinder. Iemand die begrijpt wat de organisatie écht nodig heeft – soms nog vóór de organisatie het zelf doorheeft. Die niet alleen denkt in processen, maar in mensen. In belangen. In betekenis. Functioneel beheer is dan geen taak, maar een houding: een mindset waarin waarde toevoegen voor de gebruikersorganisatie centraal staat.

Van uitvoeren naar bijdragen

Functioneel beheerders die echt van waarde zijn, pakken regie. Ze voelen zich verantwoordelijk voor de informatievoorziening als geheel, niet alleen voor hun stukje. Ze nemen initiatief, stellen kritische vragen, en houden de bedoeling van het systeem en het proces scherp in het vizier.

Dat betekent ook: durven afwijken. Niet elke situatie laat zich vangen in een standaardwerkwijze of protocol. Soms vraagt het vak om improvisatie, empathie of gewoon gezonde verstand. Juist daarin toont zich vakmanschap.

Werken vanuit een mindset

Functioneel Beheer vraagt meer dan vaardigheden en proceskennis. Het vraagt om een houding. Een manier van denken en handelen die steeds opnieuw uitgaat van: wat heeft deze situatie nodig, en hoe kan ik daaraan bijdragen? Dat is wat ik bedoel met werken vanuit een mindset.

Groeimindset: jezelf blijven ontwikkelen

Als ik het heb over mindset, bedoel ik in het bijzonder een groeimindset. Dit is het geloof dat je jezelf voortdurend kunt ontwikkelen. Niet omdat je alles al weet of kunt, maar omdat je bereid bent te leren, te proberen, te reflecteren en te groeien. Juist dat maakt het verschil in een vak dat draait om mensen, systemen en veranderingen.
In tegenstelling tot een vaste mindset ("ik ben hier nou eenmaal niet goed in"), zegt een groeimindset: "Ik kan dit leren. Misschien nu nog niet, maar wel op termijn." Fouten worden dan leermomenten. Feedback wordt iets om naar te vragen. En verandering wordt niet bedreigend, maar juist een kans om beter aan te sluiten op de behoefte van gebruikers.

Deze mindset helpt je als functioneel beheerder:

- Veerkrachtig om te gaan met verstoringen, tegenstrijdige belangen en onduidelijke situaties.
- Betrokken en nieuwsgierig te blijven, ook als het werk complex of stroperig is.
- Beter te presteren doordat je jezelf blijft verbeteren – niet uit plicht, maar uit intrinsieke motivatie.
- Open te staan voor innovatie en het gebruik van nieuwe technieken, zoals AI of datagedreven besluitvorming.

Zo werk je aan je mindset

Een groeimindset ontwikkel je niet in één dag. Maar elke dag kun je kiezen om iets kleins anders te doen. Bijvoorbeeld:

- Zie uitdagingen als oefenmateriaal. Moeilijke gebruikersvraag? Nieuwe release? Dit is jouw kans om te leren.
- Sta stil bij fouten. Niet om jezelf af te rekenen, maar om te begrijpen wat je anders kunt doen.
- Vraag om feedback. Niet als beoordeling, maar als hulpmiddel om beter te worden.
- Blijf nieuwsgierig. Stel vragen, ook als je denkt dat je het antwoord al weet.

Je mindset beïnvloedt hoe je met je werk omgaat – en dus ook hoe je overkomt op collega's, gebruikers en management. Vanuit een groeimindset ben je geen "reactieve uitvoerder", maar een professionele gesprekspartner die meedenkt, vooruitkijkt en het verschil maakt.

Leidende principes in plaats van dichtgetimmerde processen

De praktijk leert dat veel organisaties doorschieten in het vastleggen van processen. Wat begint als een hulpmiddel om grip te krijgen, mondt al snel uit in een bureaucratisch moeras waarin niemand zich nog eigenaar voelt van het resultaat.
Daarom is het tijd om de balans te herstellen: van procesgericht naar principe gedreven werken. Processen zijn belangrijk, maar ze moeten ondersteunen – niet belemmeren.
Leidende principes bieden richting zonder te verstarren. Denk aan principes als:

- De gebruiker centraal, altijd.
- Waarde boven volledigheid.
- Begrip gaat voor beleid.
- Beter één goede vraag dan tien vinkjes.

Deze principes helpen om keuzes te maken die passen bij de situatie, zonder de bedoeling uit het oog te verliezen.

Vakmanschap als kompas

Functioneel beheer is vakmanschap. Niet alleen omdat je over kennis moet beschikken, maar omdat je – net als een goede timmerman of verpleegkundige – de juiste inschatting weet te maken op het juiste moment. Je begrijpt het systeem én de situatie. Je hebt gevoel voor de bedoeling achter de processen.

Vakmanschap vraagt ruimte. Ruimte om zelf na te denken, om af te wijken waar dat nodig is en om te leren van verschillen. Juist daarom werk ik liever met leidende principes dan met dichtgeregelde werkinstructies. Want een functioneel beheerder die puur uitvoert, raakt zijn vakmanschap kwijt – en daarmee zijn waarde.
Vakmanschap betekent ook: blijven leren, goed georganiseerd zijn, je

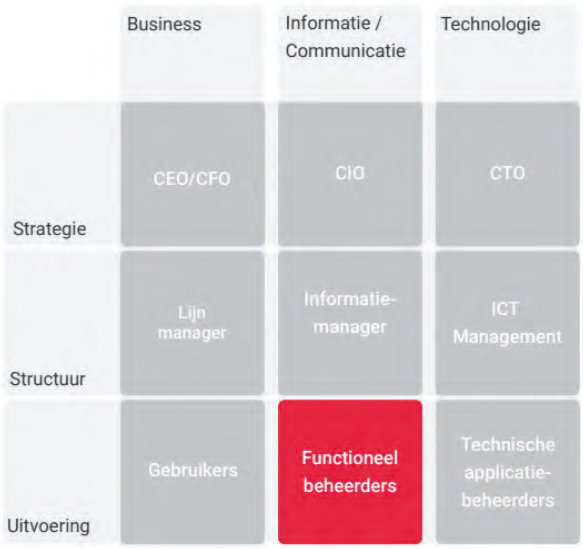
Vakmanschap geen luxe maar je kompas

vak bijhouden en werken vanuit waarden. Zoals in de zorg geldt: er is geen handboek dat elke context zo goed op waarde kan schatten als het oog, het brein en de intuïtie van een vakmens. Dat geldt net zo goed voor functioneel beheerders.

In een vak waar samenwerking, verandering en betekenis centraal staan, is vakmanschap geen luxe, maar je kompas.

En waar ligt nu de link met onze sector?

Functioneel Beheer is cruciaal voor de Nederlandse IT- en bedrijfssector. Juist ons land biedt – met zijn bedrijfscultuur, de vooruitstrevende IT-educatie, haar innovatief vermogen en het baanbrekend werk van deskundigen – kansen voor functioneel beheerders. De noodzaak van het aanwezig zijn van deze functionarissen blijkt mede uit het navolgende 9-vlaksmodel van Rik Maes.



Afbeelding 1: het 9-vlaksmodel van Rik Maes

Zie op het operationele vlak de functioneel beheerders als de kern van informatiemanagement, als brug tussen ICT en de primaire bedrijfsprocessen. Niet voor niets in de kolom van de CIO en de informatiemanager. Daarmee is het typisch Nederlands. De onmisbare schakel tussen IT en de gebruikers, gericht op succesvolle implementatie en het gebruik van IT-systemen.

De nadruk binnen IT op compliance & governance vereist de gestructureerde inzet van functioneel beheerders om te voldoen aan de wettelijke eisen van Nederlandse regelgeving. Koppel dit aan de professionele educatie & certificering voor Functioneel Beheer en duidelijk wordt de potentiële sleutelrol van deze functionarissen. Binnen Nederland schat men het aantal dan ook op 80.000 functioneel beheerders.

In het buitenland worden de taken van functioneel beheer eveneens uitgevoerd, echter per land en organisatie verschilt het daar in benaming, structuur en aanpak. In het buitenland is dus sprake van implementatieverschillen. Daar zijn business- & systeemanalisten, IT-project- & IT-Servicemanagers alsook de producteigenaar actief met afstemming tussen IT-systemen en bedrijfsprocessen. Dat richting de gebruikers echter, met variërende taken & verantwoordelijkheden buiten het domein van het functioneel beheer.

Functioneel Beheer is daardoor niet alleen typisch Nederlands, maar ook hét domein waarin wij naar verwachting zullen uitblinken en innoveren. Een status gebaseerd op onze organisatieculturen, structuren en ons onderwijslandschap. Samengevat: een resultaat van onze historie, culturele waarden en educatie. Dat vraagt om bewustwording van deze rol.

Tot slot: geen rol, maar een houding

Functioneel Beheer is geen rol die je vervult van 9 tot 5. Het is een manier van denken en werken die vraagt om betrokkenheid, lef en nieuwsgierigheid. Een mindset die begint bij de vraag: "Wat is hier nodig?" in plaats van "Wat staat er in het proces?"

Want dáár zit de kracht van ons vak: niet in de procedure, maar in de betekenis die we toevoegen. Geen trucje dus. Maar een overtuiging.

Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: ronald@eygendaal.com

De Europese Machineverordening en Cybersecurity

De Machinerichtlijn, ingevoerd in 1995, bevordert vrije handel binnen de EU en waarborgt de veiligheid van machines voor bedrijven in de Europese Economische Ruimte (EER) die machines ontwerpen, bouwen of verkopen. Een CE-markering toont aan dat een machine voldoet aan de veiligheidsnormen. Op 20 januari 2027 treedt de nieuwe Machineverordening (EU) 2023/1230 in werking, met een sterke nadruk op cybersecurity. Deze verordening stelt strengere eisen aan verbonden machines, AI-systemen en veiligheidscomponenten om cyberrisico's, zoals aanvallen op industriële controlesystemen, te minimaliseren.

CE-markering en Machineverordening

De Machineverordening behoudt de verplichting om conformiteit aan te tonen en sluit aan bij andere EU-wetgeving, zoals de Cyber Resilience Act, die brede cybersecuritynormen stelt. De verordening richt zich op machines die door digitalisering fysieke of datagerelateerde schade kunnen veroorzaken, zoals complexe machines met mechanische, bouwkundige en geautomatiseerde componenten. Fabrikanten kunnen al vóór 2027 een EU-conformiteitsverklaring afgeven. Cybersecurity-eisen zijn vastgelegd in Bijlage III, met name in paragraaf 1.1.9 ("Bescherming tegen corruptie"), die vereist dat machines bestand zijn tegen kwaadwillige manipulatie.

Cybersecurity-eisen

De Machineverordening stelt specifieke eisen aan cybersecurity:

- Risicobeoordeling: fabrikanten moeten fysieke en cyberdreigingen analyseren, vooral bij AI-systemen met zelflerend gedrag.
- Beschermingsmaatregelen: machines moeten beveiligd zijn tegen netwerkaanvallen en softwaremanipulatie. Fabrikanten moeten cybersecurity waarborgen voor minimaal 10 jaar na marktintroductie, inclusief het loggen van cyberincidenten.
- CE-markering: digitale veiligheidscomponenten en software moeten voldoen aan cybersecurity-eisen, vooral in industriële netwerken waar kwetsbaarheden fysieke gevaren kunnen veroorzaken.
- Mens-machine-interactie: bij AI- of robotsystemen moet cybersecurity veilige interactie tussen mens en machine garanderen, in lijn met de EU AI Act.

Niet-naleving kan leiden tot boetes of marktverboden.

Impact op industrie, fabrikanten, gebruikers en IT

Met de nieuwe Machineverordening, de aankomende NIS2-richtlijn en de geplande Cyber Resilience Act is cybersecurity een wettelijke verplichting voor fabrikanten, integrators en exploitanten van machines. Fabrikanten moeten investeren in maatregelen zoals encryptie, toegangsbeheer en regelmatige software-updates. Dit verhoogt kosten, maar stimuleert innovatie in veilige technologieën en versterkt de concurrentiepositie op de EU-markt. Voor gebruikers en operators betekent dit veiligere apparatuur en minder risico op downtime door cyberincidenten.

Holistische Compliance

Hoewel er geen directe link is tussen machineveiligheid en informatiebeveiligingsnormen zoals ISO 27001 en IEC 62443, worden deze normen steeds relevanter voor digitale componenten van moderne machines. Zowel de Machineverordening als deze normen stellen eisen aan patchbeheer, kwetsbaarheidsbeheer en versiebeheer. Informatiebeveiliging helpt bij het beschermen van data die machines genereren of verwerken, wat cruciaal is voor verbonden systemen. Een geïntegreerde aanpak voorkomt tegenstrijdigheden in compliance en zorgt voor een samenhangend veiligheidsbeleid.

Auteur: Petter Glenstrup, werkzaam bij Arctic Wolf als Nordisk Country Manager.
Hij is bereikbaar via: petter.glenstrup@arcticwolf.com

NIS2-compliance is een voortdurend proces en geen reden tot paniek

Maak je je zorgen over de naderende implementatie van NIS2 in de Nederlandse Cyberbeveiligingswet? Dat is niet nodig. Niet omdat de implementatie in Nederland is uitgesteld tot Q2 2026 (1) en je daarom iets meer tijd hebt, maar omdat – in tegenstelling tot de hectiek rondom de invoering van de AVG destijds – niet alles in één keer perfect hoeft te zijn. Het belangrijkste is dat organisaties tijdig beginnen. NIS2 is geen verplichting die van de ene op de andere dag moet zijn afgerond, het is een weg naar structurele digitale weerbaarheid.

"Is onze organisatie klaar voor NIS2?"

Die vraag houdt al maanden directiekamers en IT-afdelingen bezig. Terecht ook, want zodra NIS2 is verwerkt in nationale wetgeving (en er dus gehandhaafd kan worden) moeten organisaties een aantal cybersecuritymaatregelen nemen, waarbij de boetes bij nalatigheid hoog kunnen uitvallen. Het ontbreekt bij organisaties echter vaak aan een integraal, actueel overzicht van systemen, netwerkverkeer en data. Met andere woorden: veel organisaties weten simpelweg niet wat er op dit moment binnen hun IT-omgeving gebeurt. En dat is een ernstig probleem – of we het nu over NIS2 hebben of niet.

NIS2 vraagt om actieve IT-security

De NIS2-richtlijn verplicht organisaties om hun IT-omgeving proactief te beveiligen. Je moet security incidenten snel kunnen detecteren en adequaat kunnen handelen. Dat vereist continue logging, 24/7 monitoring en een goede voorbereiding. Toch zien we in de praktijk dat veel organisaties aanvallen pas opmerken als het al te laat is. Een recent voorbeeld is een bedrijf waarbij een aanval pas werd ontdekt nadat het digitale lunchsysteem uitviel. De indringer zat al geruime tijd in het netwerk, zonder dat er ergens een alarm afging — pas toen de broodjes niet meer besteld konden worden viel het op. Als het kantinesysteem de rol vervult van detectiesysteem, zegt dat genoeg over het gebrek aan security monitoring.

Dit voorbeeld is geen uitzondering. Helaas komen aanvallen nog steeds regelmatig aan het licht door iets externs, zoals een losgeldeis van aanvallers of klachten van klanten over uitval. Zonder volledig inzicht in je IT-omgeving werk je in feite blind. Als een organisatie niet weet wat er allemaal gebeurt in zijn IT-omgeving, kan deze organisatie moeilijk voldoen aan de NIS2-verplichting om ernstige incidenten binnen 24 uur te melden.

NIS2: geen eindpunt, maar een doorlopend proces

Een veelvoorkomende misvatting is dat NIS2-naleving een project is met een vaste deadline. Net zoals bij de invoering van de AVG in 2018 zagen veel organisaties die datum als een eindstreep: eenmaal gehaald, dan was je klaar. Maar zo werkt het niet met digitale veiligheid. De dreigingen veranderen continu en dat vraagt om een aanpak die zich ook voortdurend blijft ontwikkelen. NIS2 draait om het structureel verbeteren van cybersecurity: implementeren, evalueren, bijsturen – een proces dat zich blijft herhalen.

In Nederland leidde de invoering van de AVG in 2018 tot grote inspanningen bij organisaties om aan de nieuwe privacywetgeving te voldoen. Volgens een rapport van Capgemini (2) dacht in 2018 nog 78% van de bedrijven klaar te zijn voor de AVG, maar een jaar later bleek slechts 28% (3) daadwerkelijk te voldoen aan de regelgeving. Dit laat zien dat veel organisaties de complexiteit en benodigde inspanningen hebben onderschat. Veel organisaties wilden het tot in de puntjes regelen, met als resultaat: stapels beleidsdocumenten in ordners, maar nauwelijks verbeteringen in de beveiliging van persoonsgegevens.

Die fout moeten we bij NIS2 niet nog een keer maken. De aandacht moet gaan naar maatregelen die écht bijdragen aan cybersecurity: netwerkmonitoring, duidelijke responsplannen, goed toegangsbeheer en trainingen voor medewerkers. Documentatie alleen houdt cybercriminelen niet tegen – de juiste cybermaatregelen wel.

Van paniek naar plan

Het goede nieuws is dat je op de dag dat NIS2 van kracht wordt nog niet alles tot in de puntjes geregeld hoeft te hebben. Wél is het belangrijk dat organisaties dan aantoonbaar stappen zetten, inclusief de manier waarop eventuele incidenten in de opstartfase worden afgehandeld. Dit mag echter geen excuus zijn om eindeloos in de voorbereidingsmodus te blijven hangen. NIS2 vraagt om concrete stappen, geen eeuwig uitstel. Rond initiatieven af, leer ervan en ga door met de volgende verbetering.

Drie stappen die helpen bij het beginnen met het voldoen aan NIS2, zijn:

1. Breng systemen, data en kritieke diensten in kaart: je kunt niet beveiligen wat je niet goed in beeld hebt.
2. Zorg voor 24/7 monitoring: of je dit nu intern regelt of uitbesteedt aan een partner, een verdachte activiteit moet direct worden gesignaleerd én aangepakt.
3. Maak een noodplan en oefen ermee: zorg dat iedereen weet wat zijn rol is, wat voor stappen genomen moeten worden en oefen deze regelmatig. Het noodplan is niet alleen een verplichting onder NIS2, maar simpelweg verstandig om te hebben. Sla het incident response plan niet op, ergens in een map op een server, maar maak het zichtbaar – bijvoorbeeld als poster op de werkvloer.

NIS2 biedt organisaties een kans om hun digitale weerbaarheid structureel te verbeteren. Gebruik de richtlijn als manier om de basis op orde te krijgen én te houden – ook als je organisatie er formeel niet onder valt. Laat de 'afvinkmentaliteit' los. De vraag zou niet moeten zijn: "Wanneer zijn we klaar met NIS2?", maar: "Hoe zorgen we ervoor dat onze cybersecurity ook over vijf jaar nog staat als een huis?". NIS2 is geen eindstation, het is een doorlopend proces dat je helpt om beter bestand te zijn tegen digitale dreigingen.

Referenties

(1) https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025D27987&did=2025D27987

(2) https://consultancy.nl/nieuws/17883/kwart-bedrijven-tegen-jaarwisseling-nog-altijd-niet-klaar-voor-gdpr-avg

Auteur: Stijn Eijkman is mede-eigenaar van Vestingborg BV, Uw Partner voor Informatiebeveiliging en Kwaliteit. Hij is bereikbaar via seijkman@vestingborg.nl

Pragmatische implementatie van ISO 27001 bij het midden- en kleinbedrijf

Kleinere bedrijven staan voor de uitdaging om gevoelige informatie te beschermen met vaak beperkte middelen, terwijl zowel cyberincidenten als het ontbreken van aantoonbare informatiebeveiliging grote gevolgen kunnen hebben voor bedrijfscontinuïteit en reputatie.

ISO 27001 is essentieel voor bedrijven omdat het een gestructureerd informatiebeveiligingsbeleid levert om risico's effectief te beheersen en de integriteit van gegevens te waarborgen. De norm is daarnaast een strategisch verkoopinstrument dat vertrouwen opbouwt en vaak een noodzakelijke voorwaarde is voor contracten. De implementatie is ook voor kleinere bedrijven realiseerbaar door een kostenbewuste en 'lean' aanpak met standaard templates en beperkte consultancy, waardoor het haalbaar is met een beperkt budget. Cruciaal is dat de focus ligt op efficiëntie en onderhoudsgemak: door het gebruik van centrale platforms en simpele documentatie wordt bureaucratie voorkomen en blijft het ISMS als continu beheersproces actueel.

Het invoeren van een goed informatiebeveiligingsbeleid op basis van de internationaal erkende ISO 27001-norm biedt juist voor deze MKB-organisaties veel profijt, omdat het een gestructureerde aanpak biedt om risico's te beheersen en informatie effectief te beschermen. Bovendien fungeert een ISO 27001-certificaat als een internationaal erkend keurmerk dat klanten, opdrachtgevers en partners overtuigt van de volwassenheid van je informatiebeveiliging, wat in aanbestedingen en bij nieuwe opdrachten een steeds belangrijkere voorwaarde is om in aanmerking te komen.

Om succesvol te zijn met beperkte middelen, is een kostenbewuste en 'lean' aanpak cruciaal. Dit wordt bereikt door slim gebruik te maken van standaard templates en door slechts beperkt externe consultancy in te schakelen. Deze strategie maakt het mogelijk om snel een kant-en-klare basis te vullen met de eigen bedrijfsprocessen, wat onnodige overhead voorkomt. Ook is de basis gelegd voor een effectieve implementatie van bijvoorbeeld ISO 9001 of ISO 14001 (1).

De Vier Belangrijkste Redenen voor ISO 27001

ISO 27001 is een internationaal erkend kader dat organisaties helpt om informatiebeveiliging op een aantoonbare, systematische en duurzame wijze in te richten. Er zijn meerdere dwingende argumenten om deze norm te implementeren, waarbij de prioriteiten per organisatie verschillen:

1. **Gegevensbeveiliging en Risicobeheer:** de norm helpt bij het beschermen van gegevens door processen te verbeteren en risico's te beheren. Dit omvat het **systematisch detecteren van kwetsbaarheden**, het beheersen van IT-risico's, het verkleinen van de risico's op beveiligingslekken, en het minimaliseren van mogelijke schade en vervolgkosten. Bovendien waarborgt het de vertrouwelijkheid van informatie (1)(2).
2. **Wettelijke Conformiteit en Kostenreductie:** ISO 27001 draagt bij aan de naleving van wettelijke regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Het biedt een gestructureerde methode om aan deze en andere internationaal erkende conformiteitseisen te voldoen. Door risicobeheer te verbeteren, verkleint men de kans op een datalek en kunnen boetes worden vermeden, wat bijdraagt aan lagere kosten (3) (4).
3. **Reputatie en Concurrentievoordeel:** de certificering verbetert de reputatie van de organisatie doordat wordt aangetoond dat de noodzakelijke stappen zijn gezet om gegevens te beschermen. Dit verhoogt het vertrouwen van partners, klanten en het publiek, en versterkt zakelijke relaties. Door deze erkende norm te voeren, onderscheidt de organisatie zich van concurrenten, wat een concurrentievoordeel oplevert (5).
4. **Operationele Efficiëntie:** operationele voordelen omvatten de mogelijkheid tot het veilig uitwisselen van gevoelige informatie met partners en klanten. Ook draagt het bij aan een hogere productiviteit door duidelijkheid te scheppen over wie voor welke informatie verantwoordelijk is, waardoor efficiënter gewerkt kan worden (5).

Deze argumenten – betere processen, risicovermindering, compliance, vertrouwen en commercieel voordeel – komen in vrijwel elk succesvol certificeringstraject terug.

Drijfveren en Rolverdeling bij Implementatie

Bij de introductie en implementatie van een Informatie Security Management Systeem (ISMS) binnen een klein bedrijf spelen verschillende rollen met hun eigen motivering een essentiële rol. Het is essentieel om deze verschillende perspectieven te begrijpen voor een succesvolle implementatie met voldoende draagvlak:

- Commercieel Directeur: voor deze rol is ISO 27001 primair een strategisch verkoopinstrument. Het certificaat is vaak noodzakelijk om nieuwe opdrachten te verwerven of bestaande relaties te behouden, aangezien zakelijke klanten en aanbestedingen informatiebeveiliging als contractvoorwaarde stellen.
- Operationeel Directeur (COO): de COO ziet de norm als een solide kader voor de operatie. De invoering van een ISMS kan operationele processen, zoals documentbeheer en bedrijfscontinuïteit, verbeteren. Dit vereist echter wel een extra tijdsinvestering voor

zaken als audits, documentatie en trainingen. De norm dwingt tot betere procedures en duidelijkere verantwoordelijkheden en vereist een cultuur van voortdurende verbetering in plaats van een incidentele inspanning.

- Projectmanager/Consultant: bij het gebrek aan voldoende interne capaciteit wordt vaak een externe projectleider ingeschakeld. De focus van de consultant ligt op efficiëntie en onderhoudsgemak. De implementatie moet zo effectief mogelijk verlopen, en de documentatie moet zo simpel mogelijk zijn om de opvolging te vereenvoudigen. Het motto in dit proces is "keep it simple": processen, verantwoordelijkheden en systemen moeten helder, toegankelijk en bij voorkeur in één centrale omgeving worden vastgelegd. Dit waarborgt eenvoudige opvolging en continuïteit.
- Medewerkers: alle medewerkers spelen een fundamentele rol in het functioneren van het ISMS. ISO 27001 benadrukt dat informatiebeveiliging niet alleen een taak van IT is, maar van iedereen binnen de organisatie. Medewerkers moeten zich bewust zijn van het beleid, de procedures kennen en hun dagelijkse werkzaamheden uitvoeren in overeenstemming met vastgestelde richtlijnen. Hun gedrag — zoals het rapporteren van incidenten, het veilig omgaan met data of het volgen van trainingen — draagt direct bij aan het succes van het ISMS en de continuïteit van de beheersmaatregelen.

Hoewel de drijfveren per rol verschillen, benadrukken ze gezamenlijk het belang van een 'lean' implementatie. De gekozen aanpak moet voldoende structuur bieden voor vertrouwen, compliance en commerciële waarde, zonder te leiden tot onnodige bureaucratie of verspilde middelen. Dit betekent slim gebruikmaken van standaarden, hergebruik van bestaande processen en het inzetten van een centraal platform voor beheer en documentatie.

Het ISMS binnen ISO 27001

Binnen de ISO 27001-norm vormt het Information Security Management System (ISMS) het centrale raamwerk voor het beheersen van informatiebeveiliging. Een ISMS is een **systematisch en risicogebaseerd geheel van beleid, processen, procedures en beheersmaatregelen** waarmee een organisatie informatie-risico's identificeert, beoordeelt, behandelt en continu verbetert, zodat de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens gewaarborgd zijn. Het ISMS helpt organisaties om niet slechts ad-hoc reacties op incidenten te geven, maar om informatiebeveiliging structureel in de dagelijkse bedrijfsvoering te integreren en te borgen (1).

ISO 27001 gebruikt hiertoe de **gemeenschappelijke structuur voor ISO-managementsystemen** zoals vastgelegd in **Annex L**. Dit vaste raamwerk omvat de essentiële onderdelen van een managementsysteem, zoals context en scope, leiderschap, planning, ondersteuning, uitvoering, prestatie-evaluatie en verbetering (1).

Kernonderdelen van een ISMS

ISO 27001 schrijft de volgende elementen voor die, samen met de risicoanalyse en continue verbetering, samen het ISMS vormen (1):

- **Managementsysteemvereisten (ISO 27001 clauses 4–10):** deze hoofdstukken omvatten respectievelijk: context van de organisatie, leiderschap, planning, ondersteuning, uitvoering, prestatie-evaluatie en verbetering.
- **Risicobeoordeling en risicobehandeling:** systematisch bepalen wat de risico's zijn en welke maatregelen passend zijn.
- **Ondersteunende documentatie:** beleid, processen, werkinstructies en andere ondersteunende documenten.
- **Controls (Annex A):** een catalogus met 93 mogelijke controls om risico's te mitigeren, gerangschikt in vier thema's: organisatorisch, menselijk, fysiek en technologisch.
- **Registraties en auditrapportages:** vastlegging van controles, afwijkingen, audits en verbeteracties.
- **Management reviews**: periodieke evaluatie door de directie van effectiviteit en voortgang van het ISMS. Dit is een formele bespreking waarbij onder andere de voortgang, beveiligingsincidenten, auditresultaten en verbeterpunten worden bekeken. Doel is strategische bijsturing en het aantonen van commitment van de directie, waardoor het ISMS verbonden blijft met de bedrijfsstrategie.

ISO 27001 maakt gebruik van de gemeenschappelijke structuur voor ISO-managementsystemen (Annex L), wat inhoudt dat onderdelen zoals context, scope, planning en verbetercyclus vergelijkbaar zijn met andere normen zoals ISO 9001 of ISO 14001. Hierdoor worden processen als risicomanagement, interne audits en management reviews herbruikbaar in geval van uitbreiding met andere normen (1).

PDCA – De motor van het ISMS

Een kenmerk van het ISMS is dat het **geen incidenteel project is,** maar een **continu werkend systeem** dat periodiek wordt beoordeeld en aangepast. Dit wordt ondersteund door de PDCA-benadering (Plan-Do-Check-Act) van ISO 27001 (1) (6), die borgt dat informatiebeveiliging dynamisch blijft meebewegen met veranderende risico's, technologieën en bedrijfsdoelen:

1. **Plan-fase:** in deze fase worden de risicoanalyse uitgevoerd, informatiebeveiligingsdoelstellingen vastgesteld en de **V**erklaring **v**an **T**oepasselijkheid (**VvT**) opgesteld met de te implementeren beheersmaatregelen.
2. **Do-fase:** de in de VvT gekozen controls uit Annex A worden geïmplementeerd en medewerkers worden getraind om de maatregelen effectief toe te passen.
3. **Check-fase:** de effectiviteit van het ISMS wordt periodiek gecontroleerd via interne audits, monitoring en de directiebeoordeling.
4. **Act-fase:** op basis van deze evaluaties worden afwijkingen en non-conformiteiten gecorrigeerd en verbetermaatregelen doorgevoerd, zodat het ISMS continu verbetert.

Deze cyclische en gestructureerde aanpak zorgt ervoor dat het managementsysteem **levend blijft** en zich kan **aanpassen aan veranderende risico's en eisen**. Belangrijke aandachtspunten hierbij zijn:

- ISO 27001 vereist dat er een **controleschema** wordt ingericht om periodiek alle elementen van het ISMS te toetsen en assessments uit te voeren, zodat je weet dat alles blijft werken zoals gepland (6).
- Incidentbeheer en wijzigingsbeheer zijn integraal onderdeel van de PDCA-cyclus omdat ze bijdragen aan continue verbetering en risicobeheersing. Incidentbeheer richt zich op het tijdig detecteren, melden, analyseren en oplossen van beveiligingsincidenten, waarna de geleerde lessen worden gebruikt om processen en controls te verbeteren. Wijzigingsbeheer zorgt ervoor dat veranderingen aan systemen en processen gecontroleerd worden gepland, beoordeeld, getest, geautoriseerd en gemonitord, zodat risico's beheerst blijven en de integriteit van het ISMS behouden blijft tijdens opeenvolgende PDCA-fasen (6).
- Om de voortgang en samenwerking te borgen, is het aan te bevelen om een **periodiek securityoverleg** in te richten met alle betrokkenen, met een vaste agenda en actielijst om ontwikkelingen te bespreken en acties op te volgen.

Controls en de Verklaring van Toepasselijkheid (VvT)

ISO 27001 bevat in Annex A een catalogus van 93 controls die men kan toepassen om geïdentificeerde risico's te mitigeren. De organisatie bepaalt via de risicoanalyse welke maatregelen relevant zijn. De VvT beschrijft met onderbouwing welke controls zijn gekozen en welke zijn uitgesloten. Het vormt daarmee een verbindend document tussen risicoanalyse en implementatie (1) (2) (6).

De controls kunnen ook gekozen worden op basis van **contractuele of wettelijke eisen**, of omdat ze in de praktijk als best practice gelden. Dit zorgt ervoor dat het ISMS maatwerk blijft en aansluit bij de specifieke context en het risicoprofiel van de organisatie.

Efficiëntie door Tooling en Templates

Om de implementatie en onderhoudskosten laag te houden, zeker bij kleinere organisaties, zijn gestandaardiseerde templates en softwareplatforms zeer nuttig.

Een kant-en-klaar ISO 27001-template biedt een basisstructuur inclusief voorbeeldprocedures en beleid, waardoor organisaties snel van start kunnen. Een dergelijk template bevat doorgaans alle verplichte elementen, zoals beleid, formats voor managementreviews en risicoanalyseformulieren. Het is echter cruciaal dat deze generieke teksten worden aangepast en verrijkt met de concrete afspraken en processen van het eigen bedrijf. Kleine organisaties vullen zo'n template aan met hun eigen HR- en IT-processen en voegen alleen specifieke werkinstructies of controles toe die voortvloeien uit de risicobeoordeling (6).

Ook een centraal samenwerkingsplatform of wiki versnelt zowel het onderhoud als de implementatie. Dit dient als de centrale plek voor alle ISMS-documentatie en actiepunten. Dit zorgt ervoor dat medewerkers eenvoudig toegang hebben tot actuele procedures en beleid, en het voorkomt dat informatie lokaal gaat "verstoffen". Een goed opgezet platform kan taken automatiseren, zoals voortgangsrapportages en reviewafspraken, wat de samenwerking bevordert en het ISMS actueel houdt doordat auditresultaten, incidentmeldingen en documentwijzigingen inzichtelijk en navolgbaar zijn.

Succesfactoren: Leiderschap, Cultuur en Communicatie

Een succesvolle ISO 27001-implementatie is afhankelijk van actieve betrokkenheid van het management en een sterke beveiligingscultuur.

Topmanagement moet **daadwerkelijk leiderschap en commitment tonen** voor het Information Security Management System (ISMS). Dit betekent dat het informatiebeveiligingsbeleid en de doelstellingen integraal worden ondersteund en afgestemd op de bedrijfsstrategie, en dat er voldoende middelen — tijd, budget, personeel en tools — beschikbaar worden gesteld voor implementatie en onderhoud.

Door actief te **communiceren** over het belang van informatiebeveiliging en successen te delen, creëert de directie een cultuur waarin beveiliging serieus wordt genomen en gedragen door de hele organisatie. Niet alleen tijdens de implementatie, maar ook daarna, zodat het hele team begrijpt waarom de certificering nodig is en hoe het hen helpt.

Zonder dit mandaat en voorbeeldgedrag bestaat het risico dat het ISMS stagneert omdat noodzakelijke beslissingen, middelen of veranderingen niet worden geïnitialiseerd of gedragen door de organisatie.

Regelmatige trainingen, nieuwsbrieven en bijeenkomsten houden informatiebeveiliging op de agenda en ondersteunen deze aanpak.

Als **lessons learned** kunnen worden genoemd:

- Leg collega's uit wat ISO 27001 oplevert om **draagvlak** te creëren.
- Toon de **toegevoegde waarde** door te laten zien dat het ISMS het dagelijkse werk makkelijker maakt.
- Blijf inzetten op continue **bewustwording**, want informatiebeveiliging is een marathon, geen sprint.
- **First time right**: neem vanaf het begin de juiste beslissingen bij implementatie van het ISMS.
- Implementatie en onderhoud van ISMS is **teamwork**. Goede samenwerking met sleutelfiguren (HR, IT, sales) zorgt ervoor dat het ISMS aansluit bij de dagelijkse praktijk en realistisch en praktisch uitvoerbaar is. Door de kennis en het mandaat van verschillende afdelingen te benutten, wordt beveiliging de **gezamenlijke verantwoordelijkheid** van alle collega's.

Het Certificeringstraject en Continuïteit

ISO 27001 is geen eenmalige prestatie, maar een continu beheersproces, gestructureerd rond een **vaste driejarige auditcyclus** (2). Dit garandeert dat het ISMS actief wordt onderhouden volgens het PDCA-principe. De cyclus verloopt als volgt:

1. **Jaar 1: Initiële Certificeringsaudit:** deze audit bestaat uit twee fasen. Fase 1 beoordeelt de compleetheid en opzet van het ISMS (documentbeoordeling). Fase 2 beoordeelt de praktische werking en naleving van alle processen en beheersmaatregelen (implementatiebeoordeling). Bij een positief resultaat wordt het certificaat voor drie jaar toegekend.
2. **Jaar 2 en 3: Tussenaudits (Surveillance Audits):** dit zijn verplichte, minder uitgebreide jaarlijkse controles. De focus ligt op het aantonen van het continue onderhoud van het ISMS, het opvolgen van eerder vastgestelde afwijkingen, en het uitvoeren van essentiële processen zoals de Directiebeoordeling en Interne Audits. Als deze succesvol zijn, blijft het certificaat geldig.
3. **Einde Jaar 3/Begin Jaar 4:** hercertificeringsaudit: Dit is opnieuw een uitgebreide audit, vergelijkbaar met Fase 2. Hier wordt de algehele volwassenheid en effectiviteit van het complete ISMS getoetst. Bij goedkeuring wordt de cyclus verlengd en begint deze opnieuw.

De driejarige cyclus verzekert belanghebbenden dat de organisatie informatiebeveiliging ziet als een continu beheersproces en niet als een tijdelijk project. De norm vereist hiervoor het plannen van voortdurende interne audits en management reviews.

Een ISO 27001-certificaat brengt blijvende financiële en structurele verplichtingen met zich mee. Organisaties moeten jaarlijks budget reserveren voor onderhoud. Dit omvat de jaarlijkse interne en externe audits, de kosten voor tools voor monitoring en de tijdsinvestering van medewerkers voor procesverbeteringen en risicorondes. De norm vereist dat men leert van fouten; elke geconstateerde non-conformiteit of beveiligingsincident moet leiden tot corrigerende maatregelen en bijstelling van beleid of processen. Het ISMS moet consistent en gestructureerd worden onderhouden om het beoogde beveiligingsniveau op peil te houden.

Verband met Andere Normen en Wetgeving

Dankzij de gemeenschappelijke Annex L-structuur van ISO-managementsystemen is het voor een klein bedrijf relatief eenvoudig om processen zoals risicomanagement, interne audits en managementreviews; te hergebruiken voor andere normen ,zoals: **ISO 9001 (kwaliteit), ISO 14001 (milieu) of ISO 27701 (privacy)**, zodat de investering in je ISMS meerdere rendementen oplevert (1) (7).

Hoewel ISO 27001 een solide en internationaal erkend fundament legt voor informatiebeveiliging, gaat wet- en regelgeving zoals de **Cyberbeveiligingswet** en Europese **NIS2-richtlijn** verder met verplichte governance-, zorg- en meldplichten voor organisaties die daartoe behoren; ISO 27001 helpt je dan veel voorbereidend werk al op orde te hebben, maar de specifieke wettelijke eisen moet je apart in kaart brengen, zeker als je levert aan klanten die onder die regels vallen (4) (5). Daarnaast kunnen opdrachtgevers specifieke attestaties zoals **SOC 2-rapportages** vragen als bewijs van beheersmaatregelen, vooral in internationale IT-ketens.

In al deze gevallen blijft ISO 27001 waardevol als basis, maar het loont ook te bekijken welke aanvullende **markt- of juridische vereisten** relevant zijn voor jouw bedrijf — want een solide informatiebeveiligingsbeleid opent niet alleen deuren, het houd je ook klaar voor wat er op je afkomt, óók als klein bedrijf (7).

Referenties

1. NEN: Alle info over de ISO-normen en de Annex-L structuur:
   - https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging
   - https://www.nen.nl/veelgestelde-vragen-over-iso-iec-27001
   - https://www.nen.nl/nen-en-iso-iec-27001-2023-en-313608
   - https://www.nen.nl/managementsystemen
2. Duijnborgh Certification: het certificatieproces: https://dbcert.nl/
3. Autoriteit Persoonsgegevens: onderwerpen als AVG en Privacy: https://www.autoriteitpersoonsgegevens.nl
4. Digitale Overheid: Digitale wetgeving en richtlijnen: https://www.digitaleoverheid.nl
5. Ondernemersplein: Informatie en advies van de overheid voor ondernemers: https://ondernemersplein.overheid.nl
6. Instant27001: ISO 27001 norm template: https://instant27001.com/nl/
7. Implementatie ISO 27001 en ISO 9001 bij ViPcom BV: https://www.vipcom.nl

COLUMN NICOLE

Van kraamzorg tot cybersecurity: het gevaar van standaardadvies

Afgelopen oktober was het moment daar: ik werd moeder. De eerste dagen na de geboorte, half verblind door slaapgebrek, werd ik overspoeld door advies. Allemaal goedbedoeld, allemaal overtuigend, maar regelmatig tegenstrijdig en soms ronduit verkeerd.

Na de eerste week kwam ik langzaam tot de ontdekking dat de adviezen die ik kreeg – van de verloskundige, de kraamzorg, het internet – niet altijd correct waren voor mijn situatie. Hoe overtuigd iemand ook klinkt, dat maakt een advies nog niet juist voor iedereen. Daardoor kun je vastlopen, omdat je het verkeerde pad op wordt gestuurd, terwijl de juiste mogelijkheid juist wordt uitgesloten. En zo verlies je tijd.

Wat ik al snel merkte: veel adviezen gaan uit van de standaardsituatie. Het standaardkind, het standaardpatroon, het standaardprobleem. Maar wat als jouw situatie níet in dat standaardplaatje past? Dan sluit je mogelijkheden uit omdat de 'expert' zegt: "Nee, dát is het niet." "Je baby huilt niet omdat ze honger heeft. Grijp niet te snel naar de fles."

En omdat zij zo zeker klinken, ga je zelf twijfelen. Totdat je ontdekt dat het tóch zo was — dat je baby aan het afvallen is en dus onvoldoende voeding kreeg. Dat het antwoord al die tijd gewoon bovenaan je lijst stond, maar onzichtbaar werd omdat iemand anders het onmogelijk verklaarde.

Dat is misschien wel het meest onderschatte risico: niet dat je het verkeerde scenario over het hoofd ziet, maar dat je de juiste mogelijkheid zelf uitsluit, omdat een autoriteit dat al voor je deed. De blinde vlek ontstaat dan niet door een gebrek aan opties, maar door te veel vertrouwen in de aanname van een ander.

En die gedachte liet me niet los. Als dit in het ouderschap zo makkelijk gebeurt, waarom zou het in cybersecurity anders zijn? Ook in die wereld werken we met aannames, standaarden en experts die soms iets te snel iets wegwuiven. Organisaties krijgen adviezen vanuit frameworks, scans, leveranciers, auditors en consultants — vaak gestoeld op gemiddelde situaties: het 'gemiddelde' risico, het 'gemiddelde' proces, de 'typische' volwassenheidsfase.

Maar niet alle organisaties zijn gemiddelden — net als baby's, en hun moeder al helemaal niet. Elke organisatie is een eigen ecosysteem, met unieke afhankelijkheden, uitzonderlijke kwetsbaarheden en patronen die zelden netjes binnen de lijnen passen.

En precies dáár gebeurt hetzelfde als bij ouderschap: een risico of kwetsbaarheid is een mogelijkheid – hoe onwaarschijnlijk ook – maar wordt weggewuifd. "Dat kan het niet zijn."
En zodra een expert dat zegt, sluit je het zelf ook uit. Totdat het probleem hardnekkig terug blijft komen en je je realiseert dat het al die tijd op je eigen lijst stond, maar nét afweek van het standaardscenario.

Het risico is in beide werelden hetzelfde: je verliest tijd aan het verkeerde advies.
Niet omdat het advies slecht is, maar omdat het niet voor jóú bedoeld is — of omdat de ander jouw situatie simpelweg niet herkende.

Dus wat is mijn advies als columnist?
Niet dat we advies moeten wantrouwen of negeren.
Maar dat we nooit moeten vergeten dat wij misschien wel de uitzondering 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

Auteurs: Ellen Wesselingh LL.M. B.Eng EUR.ING werkt bij Sentyron als Senior Architect. Zij focust zich op de evaluatie en certificering van de producten die Sentyron ontwikkelt. Zij kan worden bereikt op ellen.wesselingh@sentyron.com

How to Execute Successful Evaluation Projects at the Highest Levels of Assurance?[1]

Common Criteria incorporates the concept of Evaluation Assurance Levels. They run from one (very lightweight) to seven (extremely rigorous). The levels are hierarchical; a higher level incorporates all the requirements of the previous level and some more. At the highest level, mathematical proof of all security functions is required and at the end all these security functions must be rigorously tested for their correct implementation. At this level, all intermediate stages in the development of the product to be evaluated (Target of Evaluation) must be documented.

The complete set of requirements means that it is extremely hard to execute an evaluation project at this highest level. Complex products with many security functions that must be formally verified take a lot of time. When software running on dedicated hardware is involved, testing shall include all possible states. This type of testing can only be accomplished when it is automated, but that in turn means that the test tooling must be rigorously verified too.

In this article, we start with a very simple, hardware only application: a data diode. The requirements on this type of product are described in a publicly available document (2). Because it is a hardware only product, with no customer configurable options, it is a small challenge in Common Criteria context. There are only seven Security Functional Requirements, which is an extremely low number for a security product. The low number of requirements does allow for very rigorous testing, though.

Risk analysis

The risk analysis, as described in the Security Problem Definition, shows all identified threats that the product must counter in its operational environment. If the product were to be deployed in a public space, the number of threats could explode because everyone may have access. In this case, the product is meant to be used in a high secure environment such as a data centre. Note that the risk analysis also lists the assumptions on the operational environment. If these assumptions are not met, the objectives that the product must fulfil cannot be met.

The assumptions are sort of the Achilles heel of the risk analysis. They are publicly available, but the point is that the customers should acquaint themselves with these assumptions. Out-of-scope usage introduces additional risk that is not considered in the risk analysis. This is therefore an action point for the risk owner, often a CISO.

Finally, the risk analysis describes any organisational policies that the product implements. In the case of a data diode, this is exactly the functionality of a diode: a one-way function. The unidirectionality in this case is not for electricity, but for data.

The results of the risk analysis are translated into objectives for the product and objectives for the operational environment. Finally, these objectives are translated into security requirements. These requirements provide detailed descriptions of what must be implemented in the product. There are Security Functional Requirements that describe ***what*** the product does, and there are Security Assurance Requirements that describe the rigour of the evaluation.

Product development

How the product implements the security requirements is up to the developer. The developer has to weigh other requirements such as performance and safety with the implementation of the security requirements. An example might be that parts of the product generate a lot of heat, so the design must cater for heat dissipation while at the same time not creating a covert or side channel with that heat. As this product is to be evaluated at the highest level, it must be capable to fend off Advanced Persist Threats, an adversary with infinite budget, time, and motivation.

During product development, careful consideration of the security architecture and the design specification are just as essential as the functional specification. At the highest levels of evaluation assurance, description of the internal structure and the source code or hardware drawings are also part of the evaluation. Finally, a security policy model is required. For the highest assurance level seven, this policy model must be formal.

A challenge of a different kind at these levels of assurance is the vulnerability management. This topic consists of the flaw remediation process, which must be implemented by the developer to assure that vulnerabilities are consistently reported and mediated. It also means that the developer must be capable to do a vulnerability analysis on reported vulnerabilities and provide a fix when the analysis shows a case of an actual exploitable vulnerability.

Product deployment

So, what to do when products are deployed and a vulnerability emerges? In the case of hardware, it would probably mean replacement of the hardware in the field. If the product is configurable hardware, it may be possible to instruct the user to configure it in a secure way to fix the problem, but in the case of non-configurable hardware (such as the data diode example), it is hard to imagine another solution than hardware replacement.

An example of such a recall was the payment card replacement from magstripe to chip and PIN cards in the United Kingdom at the start of this century (3).

In case the product can be fixed with a software update, it would mean a new evaluation of the product, because it has changed. Depending on the severity of the change, this may mean a maintenance evaluation or a complete evaluation. With a fix for an actively exploited vulnerability, it is hard to imagine that the impact is minor, a requirement for maintenance. However, if the security architecture is sound, it may be possible to contain the problem in a subsystem or module, reducing the size of what must be re-evaluated.

In this sense, the formal proofs required at the highest assurance level may show to be a blessing in disguise. For the proofs show the soundness of the architecture of the security functions. If that proof still holds, even after the discovery of a vulnerability, the focus of the new evaluation can be on the implementation of the security functionality. This would reduce the re-evaluation to mostly implementation, testing, and evaluator vulnerability analysis.

One other aspect that has not been touched yet, is the delivery of the product and user instruction. Let us assume that the development environment security is sound, so that the confidentiality and integrity of the product or its components are assured during development. Now, the final product must be delivered in a secure way to the customer. And the customer must know how to install it in a secure way. In our example of the data diode, the customer must know how to install the data diode such that the one-way function is implemented in the intended direction, not vice versa. And, of course, the customer must know how to verify the integrity of the product.

High assurance product development and use principles

This brings us to some key takeaways for high assurance product development and use principles. These principles are rules-of-thumb, or best practices, to avoid as much as possible elementary design mistakes that introduce vulnerabilities.

First, the well-known Keep-It-Simple-Stupid or KISS principle applies (4). At the highest evaluation level, it is even a formal requirement to reduce complexity in the architecture and design of the product. Hence, no fancy add-ons or things that are included for potential future use.

Second, stick to your risk analysis as use in product development and do not encourage out-of-bounds use of the product by your customers. From a business perspective, this may seem counter-productive, however, in the long run this policy provides trust in the product and prevents liability issues with an installed base. Product recalls and customers complaining even though they did not properly install or maintain the product are bad publicity.

Third, make sure everyone in product development (and sales!) is on the same page. This is probably the most challenging principle to implement. It means that developers understand that there are boundaries to whatever implementation they want to build, the use of secure tooling and programming languages, security minded coding standards use, and so on. This is way beyond the awareness of the average developer. It also means that the salespeople (and customers!) must understand that they cannot just ask for more functionality because a particular customer asks for it. Any request for additional functionality must go through the risk analysis process.

And finally, the customer must inform themselves about the risk analysis. Especially when this analysis is public, as is the case in our data diode example, they must take some time to read and assess it. Only if the customer uses the product in cases for which it was designed, is the added value of a product evaluated at the highest assurance level achieved.

References:

(1) This was the title of a presentation, I gave with one of my ITSEF representatives, at the International Common Criteria Conference 2025. Afterwards, there was quite some interest, hence this article. Some basic knowledge about Common Criteria, also known as ISO 15408, is assumed.

(2) Hardware Data Diode Protection Profile (Sentyron), 27 October 2025. Available at https://www.commoncriteriaportal.org/pps/index.cfm (not yet available pending the final acceptance by the certification body).

(3) Card fraud in 2004 cost £504 million in UK (Pinsent Masons), 8 March 2005. https://www.pinsentmasons.com/out-law/news/card-fraud-in-2004-cost-504-million-in-uk

(4) KISS principle (Wikipedia). https://en.wikipedia.org/wiki/KISS_principle

COLUMN PRIVACY

Mr. Rachel Marbus

Van digitale soevereiniteit tot AI-bubbels: wat staat ons te wachten in 2026?

Met de oliebollen alweer lang en breed achter de kiezen, de champagneflessen geleegd en de kerstboom op de brandstapel, is het tijd om vooruit te gaan kijken. Wat gaat er dit jaar spelen op het gebied van privacy?

Eén ding staat als een paal boven water: het debat over digitale soevereiniteit en de zoektocht naar schaalbare oplossingen gaat in een grotere versnelling komen. Veel onderzoekswerk en verkenningen zullen van universiteiten gaan komen. Verschillende van hen, waaronder de TU Delft, bundelen de krachten en ook de overkoepelende onderwijsorganisatie SURF helpt daarin mee. Zij biedt vanaf januari dit jaar de mogelijkheid aan gebruik te maken van Nextcloud, een opensource-omgeving voor tekstverwerken, documenten delen, e-mailintegratie en online vergaderen. Hoewel universiteiten daarmee niet direct van 'Big Tech' af kunnen, is het een belangrijke stap richting een digitaal soevereine toekomst.

Ook zullen we nog wel even op de AI-bubbel blijven zitten, waar in toenemende mate meer aandacht moeten komen voor awareness bij gebruikers. Daar lijkt het tot nu toe nog wat aan te ontbreken. Recentelijk ging de gemeente Eindhoven flink de mist in en ze zullen zeer zeker niet de enige zijn. Een interne steekproef toonde aan dat ambtenaren meerdere malen persoonsgegevens door LLM's (large language models) haalden, zoals ChatGPT. En daarmee pittige datalekken creërende want de persoonsgegevens die gedeeld zijn, worden vervolgens gebruikt om het AI-model mee te trainen. En daar hebben burgers en ambtenaren natuurlijk geen toestemming voor gegeven. Om te voorkomen dat het nog langer mis kan gaan, zijn alle openbare AI-websites door de gemeente geblokkeerd. Een prima oplossing voor de acute situatie, maar niet houdbaar naar de toekomst toe. Het is tijd voor awareness en regels voor het gebruik van AI binnen de eigen organisatie (ja, ook bij anderen).

Bovenstaande onderwerpen zie je ook terug bij de focusgebieden van de Autoriteit Persoonsgegevens, die in het bijzonder de pijlen richt op: 'algoritmes en AI', 'Big Tech' en 'Datahandel'. Daarbij zal AP vooral letten op: onjuiste data, foutieve aannames, uitsluiting en discriminatie, nepnieuws en politieke targeting en ongeoorloofde (door)verkoop van persoonlijke gegevens.
En, ten laatste, maar zeker niet het minst belangrijke: in de vergaderzalen en wandelgangen van de EU in Brussel en Straatsburg zal nog veel gesproken gaan worden over versoepelingen van de AVG. Die gaan eraan komen, de eerste voorstellen zijn gedaan en inmiddels ook geanalyseerd en besproken door specialisten. Wat dat precies op gaat leveren durf ik nog niet te voorspellen. Daar waar het privacywetgeving betreft, wordt doorgaans een zware lobby gevoerd door heel veel verschillende partijen en voorgestelde wijzigingen krijgen daardoor vele amendementen voor de kiezen. Het zal – hoe dan ook – een interessant jaar gaan worden.

Ik wens jullie alle moois en een privacyvriendelijk 2026!

Rachel

Auteurs: Arvid Landwaart en Jelle Hoekstra zijn mede-eigenaar van Pasquil, een adviesbureau voor informatiebeveiliging en privacy. Ze zijn bereikbaar via: hallo@pasquil.nl.

Risicomanagement: hoe doe je dat goed?

Iedereen praat erover, weinig mensen snappen hoe het werkt. Dit artikel gaat over risicomanagement. Als informatiebeveiligingsprofessional word je hier vaak mee geconfronteerd. De aandacht ervoor zal toenemen met de komst van de Cyberbeveiligingswet. De uitdaging is: hoe doe je risicomanagement goed? In dit artikel delen wij onze tips en tricks.

Veel organisaties starten vaak met een risicoanalyse, omdat het in ISO27001 of de BIO staat. Een risicoanalyse is echter nog geen risicomanagement. Een risicoanalyse is een eenmalige exercitie, terwijl risicomanagement zorgt voor continu risicogestuurd werken in je organisatie.

De theorie is dat risicomanagement leidt tot de meest effectieve en efficiënte aanpak voor informatiebeveiliging. In de praktijk wordt risicomanagement vaak te complex en daarmee tijdrovend. Het is belangrijk om risicomanagement eenvoudig te houden en als proces te zien. Dat betekent: klein beginnen, niet volledig willen zijn, het hele proces doorlopen en de scope pas uitbreiden als iedereen het spelletje snapt.

Hoe doe je dit in de praktijk? We geven hieronder concrete tips. De stappen die wij hanteren zijn: voorbereiding, identificatie, analyse, behandeling, evaluatie en rapportage.

Voorbereiding

Zorg voor duidelijkheid in definities! Risicomanagement is abstract, dat kunnen we niet verhelpen. De uitdaging is om vage termen zo concreet als mogelijk te maken. Je helpt jezelf en de organisatie door een vaste zinsopbouw te gebruiken. Wij gebruiken de volgende zinsopbouw als formule:
"(Bedreiging) misbruikt (Kwetsbaarheid), wat leidt tot (Gebeurtenis), met een (Gevolg (verlies beschikbaarheid, integriteit of vertrouwelijkheid voor informatiebeveiliging)) en gevolg voor een (proces)."

Deze formule maakt duidelijk waar het probleem in de beschreven situatie precies zit. Als dat scherp geformuleerd is, dan helpt dat bij het analyseren en evalueren van risico's.

Inventarisatie

Zorg dat risico-eigenaarschap is belegd (niet bij de CISO!). Elk risico moet een duidelijke eigenaar hebben. Door eigenaarschap te definiëren, neemt iemand binnen de organisatie verantwoordelijkheid voor het monitoren en bijwerken van het risico. Deze persoon moet wel de middelen hebben om het risico te kunnen managen. Dit geeft niet alleen focus, maar voorkomt ook dat risico's onopgemerkt blijven. Let op: een eigenaar van een risico is niet hetzelfde als de eigenaar van de maatregel! De eerste is eindverantwoordelijk voor het risico op managementniveau en de tweede is verantwoordelijk voor de uitvoering van beheersmaatregelen. Maak dit ook duidelijk aan de betreffende personen.

Gebruik goede inspiratie (niet alles zelf bedenken). Als je vanaf nul begint, dan vergeet je gegarandeerd een aantal risico's die relevant zijn voor jouw organisatie. Het helpt om te starten met een goede structuur. Denk ook aan de keuze van een schaal voor de "kans en impact matrix". Twee solide manieren om tot een lijst met risico-omschrijvingen te komen zijn: (1) vanuit Beschikbaarheid Integriteit en Vertrouwelijkheid (BIV) redeneren op basis van 'kritieke processen' of (2) vanuit risico-eigenaren/domeinen. Wij hanteren altijd aanpak twee. De overweging daarvoor is dat het risico-eigenaren betrokken houdt én praktisch is bij het plannen van risicosessies.

Naast de methode en het startpunt zijn er - voor de risico's zelf - bronnen om inspiratie uit te halen. Bekende methoden zijn **R**isico**A**nalyse **V**oor **I**nformatie**B**eveiliging (**RAVIB**) en **MAPGOOD** (**M**ensen, **A**pparatuur, **P**rogrammatuur, **G**egevens, **O**rganisatie, **O**mgeving en **D**iensten). Bij MAPGOOD ligt de nadruk wat meer op de fysieke wereld en daarom gebruiken wij dit meestal niet (voelt een beetje ouderwets, mist de invalshoek van moderne digitale dreigingen). RAVIB is een standaard lijst met risico's en biedt ook een leuke gratis tool (1). Nadeel is dat de risico's in de RAVIB set niet altijd een consequente opbouw hebben voor de risico-omschrijving. Vanuit Pasquil hebben we een aantal standaard risicosets ontwikkeld waar iedereen inspiratie uit kan halen (2).

Risicoanalyse

Doe de analyses in een fysieke setting. De analyse wordt meestal gedaan in een sessie met verschillende stakeholders. De aanwezigen zijn vaak: een risico-eigenaar, inhoudelijke experts en iemand die het proces coördineert en registreert (CISO/ISO). Het is fijn als iedereen erbij kan zijn, omdat dit zorgt voor verschillende invalshoeken en een gezonde discussie met de belanghebbenden. Dit werkt het beste tijdens een fysieke bijeenkomst, online is het lastiger om iedereen betrokken te houden.

Gebruik initiële-, huidige- en doelscore in plaats van bruto - en netto scores. In onze ervaring werken de termen bruto - en netto risicoscores verwarrend. Een bruto risicoscore bestaat alleen theoretisch (en risicomanagement was al abstract). Een bruto risicoscore (zonder maatregelen) is namelijk niet meer denkbaar, omdat veel maatregelen in organisaties 'default' aanwezig zijn. De vraag is: wat heb je praktisch aan een bruto risicoscore? Vrij weinig is onze ervaring, daarom maken wij gebruik van:

- 'Initiële risicoscore', de score die je hebt als je voor het eerst de risicoanalyse doet.
- 'Huidige risicoscore', de actuele score van het risico, die lager is dan initieel, zodra je enkele maatregelen hebt genomen (is gelijk aan 'initieel' op het moment dat je voor het eerst de risicoscore uitvoert).
- 'Doel/rest risicoscore', de risicoscore waar je naartoe wilt gaan met de voorgestelde maatregelen.

Het grootste voordeel is dat je heel mooi de status kan rapporteren van

de risicoscores door de tijd heen. Hiervoor kan de juiste tooling veel administratieve last verminderen. Wij gebruiken daar onze zelf-ontwikkelde tool Risqui voor (3).

Kies het juiste detailniveau van de risico-omschrijving. Het beschrijven van een risico op het juiste detailniveau is lastig. Het abstractieniveau ervan kan zowel te hoog als te laag zijn. Dat klinkt wat vaag, daarom geven we even wat voorbeelden.

Een te laag detailniveau is: "*Datalek*" Een te hoog detailniveau is: "*Doordat Jan vorige week vrijdag op een phishingmail had geklikt en op dat moment zijn HP Probook niet opnieuw had opgestart waardoor de update van Windows 11 business nog niet was uitgevoerd en de 16-jarige Finse hacker Jari toegang kreeg tot zijn OneDrive, wat had opgemerkt kunnen worden als het SOC-team niet net een team-uitje had en waardoor dus de sollicitatiebrief en het CV van Annie nu op straat ligt.*"

Ergens daartussenin ligt een optimum. Eigenlijk is het beste om de beschrijving zo algemeen mogelijk te houden, maar met genoeg details zodat deelnemers van de sessie een goede inschatting van de impact- en kansscore kunnen maken. Het juiste abstractieniveau van de risico-omschrijving blijft, zelfs met heel veel ervaring, altijd wikken en wegen. Het is dus logisch als je hier tegenaan loopt.

Houd de bijeenkomsten behapbaar. Het uitvoeren van een risico-workshop of risicoanalyse is pittig. Risico's zijn abstract en het vraagt veel van het analytisch vermogen. Verder is het lastig om vrolijk te blijven als je anderhalf uur over negatieve 'wat als' scenario's praat. Een goede voorbereiding helpt jouw collega's of klanten om de sessie door te komen en ook de manier waarop de sessie wordt geleid. Houd het luchtig, gebruik wat humor, neem een pauze en laat een sessie niet langer duren dan twee uur. Als je meer tijd nodig hebt, plan dan gewoon een vervolg in! Overweeg om de sessie samen met iemand anders te verzorgen: dat kan door de taken: "sessie leiden" en "de administratie voeren" te verdelen.

Risicobehandeling

Focus op te nemen maatregelen. De risicoanalyse heeft als doel dat je identificeert welke maatregelen nog moeten worden getroffen. Het is goed om inzicht te hebben welke maatregelen er al zijn en er een motivatie voor te hebben. Maak het jezelf daarbij niet te moeilijk. Bij bijna alle risico's kan je bijvoorbeeld: 'bewustwording', 'informatiebeveiligingsbeleid', 'rollen en verantwoordelijkheden' toevoegen als maatregel. Als je dat overal toevoegt ben je onnodig aan het typen. Houd dus de focus op aanvullende maatregelen en zorg dat je de maatregel specifiek maakt voor het risico. In plaats van 'bewustwording' is 'bewustwording op het herkennen en melden van phishing-mails' specifieker en daarom beter.

Laat lage risico's links liggen. Risicogebaseerd werken is keuzes maken. Dat betekent dat je lage risico's met rust moet laten en echt eerst de focus moet leggen op de hogere. Accepteer in de eerste ronde alles wat laag genoeg is en laat je niet afleiden door allerlei maatregelen te verzinnen voor deze risico's. Die kan je later, bij de evaluatie van de risico's, een keer oppakken.

Gebruik de optie van tijdelijk accepteren. De hoeveelheid werk die klaarligt na een risicoanalyse is afhankelijk van de volwassenheid van een organisatie. Als er veel hogere risico's zijn, helpt het om een aantal minder hoge risico's tijdelijk te accepteren. Hierdoor ontstaat meer tijd en ruimte voor de hoge risico's. Stel voor deze minder hoge risico's de acceptatie en de datum vast. Bij een evaluatie kan je altijd weer terugkomen op deze risico's en kijken wat je er dan mee doet of wil.

Risico-evaluatie

Het idee van een risico-evaluatie is dat je enige tijd na een eerste (of eerdere) risicoanalyse(s) opnieuw naar je risico's kijkt en de score op dat evaluatiemoment bepaalt. De meeste organisaties hebben de grootste moeite om risico-evaluaties goed uit te voeren, terwijl dit deel juist de grootste meerwaarde oplevert van al het eerdere werk wat je erin hebt gestopt! Immers: dit is het moment dat je kan zien waar je voortgang op hebt geboekt (bijvoorbeeld hoeveel risico's verlaagd) of waar je nu alsnog risico's wilt verlagen, die je eerder tijdelijk geaccepteerd had.

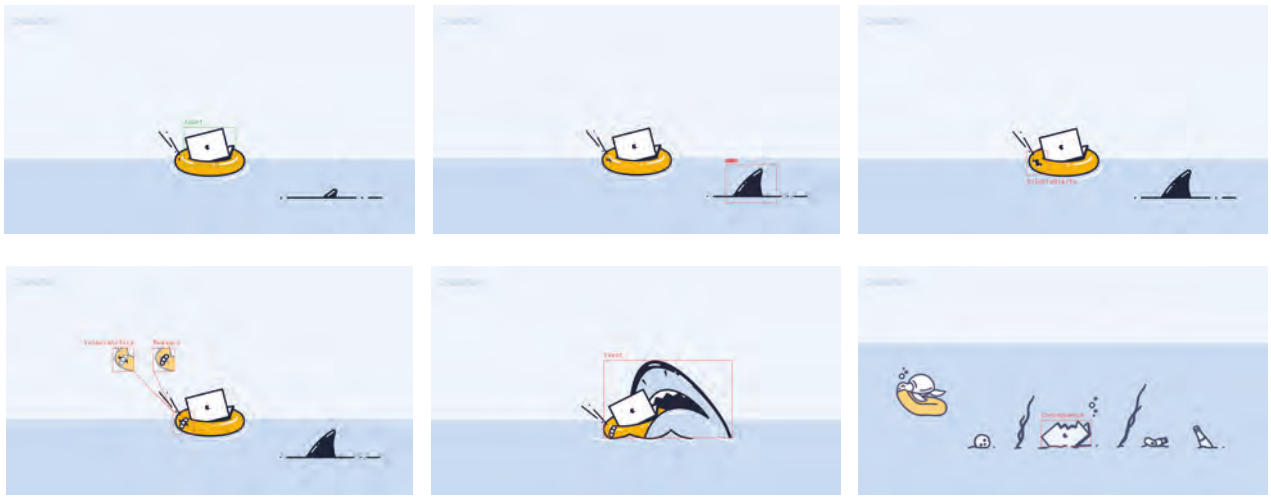
Houd zicht op de huidige risico-score en inzicht in verbetering over tijd. Risico's en risico-scores zijn niet statisch, maar veranderen (hopelijk in positieve zin) gedurende de tijd. Dit kan bijvoorbeeld gebeuren door externe factoren:

- Verandering in dreigingen.
- Nieuwe kwetsbaarheden.
- Nieuwe klanten.
- Verandering in wetgeving.

Of bijvoorbeeld door interne factoren:

- Het succesvol implementeren van een maatregel.
- Het wegvallen van maatregelen of als na controle blijkt dat een maatregel niet goed is geïmplementeerd.
- Een organisatieverandering.
- Evaluatie van kans of impact naar aanleiding van een incident.

Risico's veranderen dus. Daarom is het belangrijk om in het risico-overzicht de huidige score bij te houden en de omschrijving aan te



passen. Er komen dus mutaties op de risico's, maar dat laat juist zien dat je actief met risicomanagement bezig bent. Zo zorg je ervoor dat je inzicht hebt in de actuele risico's en waarschijnlijk bezig bent met het mitigeren van de hoogste risico's. De verandering van de scores over de tijd maken inzichtelijk (voor jezelf en voor het management) of de aanpak werkt: hoogste risico's verlagen.

Houd de risico-eigenaar betrokken. De risico-eigenaar moet iets doen met het risico en daar dus ook het ongemak van voelen. Expliciet maken van de verantwoordelijkheid, de eigenaar ook aanspreken op de voortgang alsook diens verantwoordelijkheid daarvoor; zorgt voor betrokkenheid en draagvlak van het management met betrekking tot die maatregelen. Dit werkt alleen als de risico-eigenaar wordt betrokken, regelmatig de risico's onder ogen krijgt en deze ook officieel evalueert. Natuurlijk betekent dat niet dat de risico-eigenaar elke week in het risico-overzicht moet kijken, maar elk kwartaal een deel van de risico's (bijvoorbeeld de hoge) evalueert is een goed idee.

Houd de evaluatie kort. De evaluatie van de risico's moet veel minder tijd kosten dan de initiële analyse. Als je elke keer de hele analyse gaat doorploegen, zullen de risico-eigenaren afhaken. Kijk in plaats daarvan naar het verschil in de context van het ISMS en welke incidenten er zijn geweest. Bereid de evaluatie voor met eventuele aanpassingen en mogelijke verbeteringen voor de risico's. Tijdens de evaluatie moet je vooral focussen op de hogere risico's, eventuele nieuwe risico's en controleren of de huidige scores van de hogere risico's zijn veranderd. Veranderingen in lage risico's komen alleen voort uit verandering in de context, zoals een ander dreigingsniveau of verkregen inzicht door incidenten.

Rapportage

Zorg voor een duidelijk rapportageproces. Om de risico-eigenaar betrokken te houden (en licht ongemak te laten voelen) is het noodzakelijk om doorlopend te rapporteren over de risico's. Zie jezelf als een coach, die ervoor zorgt dat je trainees met spierpijn naar huis gaan: een beetje pijn is nodig om vooruit te komen.

Een rapportage voor het management moet simpel zijn. Stop er niet te veel details in, maar zoom in op hoge risico's die aandacht behoeven. Door ook te rapporteren over het verloop van risico's over tijd, wordt voortgang inzichtelijk gemaakt. Managers worden er blij van om vakjes of bolletjes van rood (via oranje) naar groen te zien gaan. Dat laat eenvoudig de resultaten van de informatiebeveiligingsaanpak zien.

Tot slot

Er zijn in dit stuk heel wat tips gedeeld. Dit geeft je als lezer wat meer inzichten en motivatie om te starten met risicomanagement of om de aanpak te verbeteren. Dit is ook de enige manier om risicomanagement echt onder de knie te krijgen: ermee aan de slag gaan! Vraag eventueel hulp, bij een concullega of adviseur. Succes met het ervoor zorgen dat risico-eigenaren (licht) ongemak gaan voelen en uiteindelijk tot mooie resultaten komen!

Referenties

(1) https://www.ravib.nl/

(2) https://pasquil.nl/wat-doen-we/template-standaard-risicoset/

(3) https://www.risqui.nl/

Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: ronald@eygendaal.com

De jacht op straling

In september 2025 arresteerde de politie twee 17-jarige Nederlandse jongens. Ze zouden in opdracht van Rusland hackopdrachten hebben uitgevoerd. Gewapend met WiFi-sniffers liepen de tieners langs cruciale gebouwen in Den Haag, zoals het Europol-kantoor en de Canadese ambassade, om WiFi-verkeer af te tappen.

Zeven jaar eerder, in 2018, probeerden vier Russische hackers vanaf een parkeerplaats in Den Haag in te breken in het WiFi-netwerk van de Nederlandse overheid. Ook zij werden gearresteerd.

Deze incidenten laten pijnlijk zien hoe kwetsbaar de radiostraling van WiFi is bij hoogrisico-objecten. In een tijdperk waarin draadloze communicatie centraal staat in ons IT-landschap, biedt LiFi (Light Fidelity) een revolutionaire oplossing. In plaats van radiogolven gebruikt LiFi zichtbare lichtgolven, infrarood of ultraviolet licht om data over te dragen, sneller en potentieel veiliger. LiFi lost echter niet alle stralingsproblemen op. Dit artikel belicht de LiFi-technologie, de beveiligingsvoordelen en -uitdagingen, organisatorische implicaties en de integratie met TEMPEST-mitigaties, inclusief toekomstperspectieven.

Wat is LiFi

LiFi is een technologie die gebruikmaakt van LED-lampen om gegevens via licht te verzenden. Deze lampen vormen de basis van LiFi, omdat ze miljarden keren per seconde aan en uit kunnen schakelen, onzichtbaar voor het menselijk oog, om digitale informatie in binaire vorm over te dragen.

Een fotodetector, zoals een fotodiode, ontvangt deze lichtsignalen en zet ze om in elektrische signalen die apparaten kunnen verwerken. De snelheid van LiFi varieert per situatie; in laboratoriumtests zijn snelheden tot 224 gigabit per seconde (Gbps) behaald, terwijl praktische toepassingen doorgaans lagere snelheden bieden, rond 3,5 Gbps of 30 Mbit/s bij commerciële systemen. LiFi opereert binnen het zichtbare lichtspectrum en vereist een directe zichtlijn tussen de zender (LED-lamp) en ontvanger.

Dit maakt dat het licht geen muren kan doordringen, wat zowel een beperking als een voordeel is, met name voor informatiebeveiliging.

Informatiebeveiliging en LiFi

Een van de grootste voordelen van LiFi op beveiligingsgebied is de fysieke beperking van licht. Omdat lichtsignalen niet door muren of ondoorzichtige objecten heen gaan, is het veel moeilijker voor onbevoegden om van buitenaf toegang te krijgen tot het netwerk. Dit in tegenstelling tot WiFi, waarbij radiogolven over lange afstanden en door fysieke barrières heen kunnen worden opgevangen, wat het risico op afluisteren vergroot.

Bovendien zorgt LiFi voor natuurlijke netwerkisolatie. In een kantooromgeving kan elke kamer een eigen LiFi-netwerk hebben, zonder interferentie of overlapping met andere ruimtes. Dit vermindert de kans op ongeautoriseerde toegang tot gevoelige gegevens.
LiFi kan worden gecombineerd met encryptietechnieken zoals AES (Advanced Encryption Standard) om de gegevensoverdracht nog verder te beveiligen. Sinds 2025 zijn er LiFi-producten op de markt met FIPS (Federal Information Processing Standard) 140-3-certificering, waardoor LiFi nog geschikter wordt voor high-security toepassingen. LiFi is gestandaardiseerd onder IEEE 802.11bb.

Uitdagingen op het gebied van beveiliging

LiFi-hacking is een relatief nieuw en complex onderwerp, mede door de unieke aard van de technologie. Omdat LiFi gegevens via lichtsignalen overdraagt, vereist hacking een directe zichtlijn naar de lichtbron, wat het moeilijker maakt dan bij WiFi. Toch zijn er potentiële kwetsbaarheden, zoals het onderscheppen van signalen met geavanceerde optische apparatuur als de zender niet goed is afgeschermd.

Manipulatie van LED-lampen, fotodetectors of netwerkverbindingen kan theoretisch ook toegang bieden tot het netwerk. Encryptie, zoals AES en fysieke beveiliging van de infrastructuur zijn cruciaal om deze risico's te minimaliseren. Tot nu toe zijn er weinig geregistreerde gevallen van succesvolle LiFi-hacks, maar onderzoek blijft nodig naarmate de technologie groeit.

In het huidige complexe en onvoorspelbare geopolitieke landschap neemt de kwetsbaarheid toe.

Een andere uitdaging is de integratie van LiFi in bestaande netwerkinfrastructuren. Veel organisaties vertrouwen op een combinatie van bekabelde en draadloze netwerken en het implementeren van LiFi vereist investeringen in nieuwe hardware, zoals LED-lampen en fotodetectors. Daarnaast moeten organisaties ervoor zorgen dat de software en protocollen die LiFi-netwerken ondersteunen, voldoen aan strenge beveiligingsnormen om kwetsbaarheden te minimaliseren.

Toekomstperspectieven

LiFi is momenteel operationeel, vooral in sectoren waar informatiebeveiliging van groot belang is. Onderzoekers werken aan innovaties, zoals het inzetten van meerdere lichtbronnen om de dekking te vergroten en de afhankelijkheid van een directe zichtlijn te verminderen, met aandacht voor roaming tussen verschillende LiFi-netwerken. Gebruikers willen immers naadloos van hun kamer via de gang naar een andere ruimte kunnen bewegen zonder connectieverlies.

Ook wordt er aan locatiebepaling gesleuteld; in LiFi-gebouwen kunnen LED-lampen dankzij de zichtlijn je positie bepalen, waardoor lampen buiten bereik niet hoeven te zenden of te ontvangen. Daarnaast worden hybride systemen onderzocht die LiFi en WiFi integreren om zowel snelheid als beveiliging te verbeteren. Bovendien wordt LiFi al toegepast in omgevingen waar radiogolven ongewenst zijn en elektromagnetische interferentie een probleem kan vormen; hier kan LiFi de oplossing bieden.

LiFi geeft organisatorisch gedoe

De introductie van LiFi zal ook organisatorisch voor aanzienlijke verandering zorgen. Er zijn namelijk al lichtarmaturen op de markt die LiFi ondersteunen, wat een nieuwe dimensie toevoegt aan de infrastructuur van kantoren en andere werkplekken. Dit roept de vraag op: zal de IT-afdeling dan ook verantwoordelijk worden voor de verlichting? Het integreren van verlichting en internettechnologie kan leiden tot een herdefiniëring van taken binnen organisaties. Dit zou betekenen dat IT-medewerkers mogelijk training nodig hebben om met deze hybride systemen om te gaan.

Tegelijkertijd kan het de samenwerking tussen afdelingen zoals facilitair management en IT versterken. Het is een ontwikkeling die zorgvuldige planning en aanpassing vereist om soepel te verlopen.

LiFi en TEMPEST

LiFi elimineert WiFi-radiostraling, maar andere apparaten blijven lekken. TEMPEST – het onbedoeld uitzenden van elektromagnetische signalen door monitoren, toetsenborden, kabels en servers – verraadt nog steeds toetsaanslagen, scherminhoud of verwerkte data. Na de Koude Oorlog lang als verouderd beschouwd, is deze dreiging weer springlevend.

In het huidige complexe en onvoorspelbare geopolitieke landschap – gekenmerkt door oplopende spanningen, verschuivende machtsverhoudingen en miljardeninvesteringen in veiligheid en defensie – neemt de kwetsbaarheid toe.

Het snel veranderende cybersecurity-landschap heractiveert oude gevaren zoals TEMPEST. Technologische vooruitgang heeft de risico's niet verkleind, maar juist verfijnd: moderne interceptietechnieken en groeiende spionageactiviteiten maken het mogelijk om deze zwakke straling op te vangen, van enkele meters tot honderden meters ver, afhankelijk van de gebruikte apparatuur.

Hybride aanvallen

Ook de toename van hybride aanvallen, zoals spionage en cyberoperaties, maakt de Tempest relevantie groter. Staten en niet-statelijke actoren, zoals hackersgroepen, kunnen Tempest technieken combineren met andere methoden zoals social engineering of netwerkhacks om toegang te krijgen tot gevoelige systemen.

Bouwkundige beveiliging

Bij de beveiliging tegen TEMPEST speelt bouwkundige beveiliging een belangrijke rol. Een Faraday-kooi is een afgeschermde ruimte die elektromagnetische straling blokkeert. Het bouwen van zo'n kooi is geen eenvoudige klus; het vereist precisie, planning en de juiste materialen. De kern ligt in het creëren van een volledig geleidende barrière zonder onderbrekingen, goed geaard, en in staat om de specifieke frequenties van TEMPEST-signalen – variërend van kHz tot GHz – te blokkeren.

De kooi mag geen openingen hebben groter dan een fractie van de golflengte van de signalen die je wilt blokkeren – voor GHz-frequenties betekent dit openingen kleiner dan een paar millimeter. Een spectrumanalyzer of EMF-meter is onmisbaar om na de bouw te controleren of de kooi daadwerkelijk werkt. Elk detail telt: een kleine kier, een slecht geaarde verbinding, of een vergeten naad, kan de hele afschermingmaatregelen ondermijnen. Lekken in de kooi worden vaak veroorzaakt door deuren en ramen. Zo dienen ramen bedek te zijn met geleidend gaas of folie en zorgt een slechte, geleidende afdichting rond deuren vaak voor lekkage.

Geen standaard kantooromgeving

Een standaard kantooromgeving is op zichzelf geen Faraday-kooi. Gebruikers hebben immers behoefte aan een bureau, een computer, netwerkverbinding, verlichting, verwarming en andere faciliteiten. Een standaard kantoor zal aangepast moeten worden naar een Faradaykooi.

Bij de inrichting van een dergelijke kantoor ruimte gelden echter specifieke TEMPEST-eisen die in acht moeten worden genomen. Zo is het bekend dat voedings en netwerkkabels zeer gevoelig zijn voor Tempest. Om elektromagnetische interferentie (EMI) en radiofrequentie-interferentie (RFI) te voorkomen, moeten deze kabels op de overgang tussen de externe omgeving en de afgeschermde ruimte (kooi) worden voorzien van Tempest filters ter bescherming. Maar ook alle elektrische apparaten in de kooi dienen voorzien te zijn van deze filters.

Een moderne kooi van Faraday is uitgerust met een intern LiFi-netwerk. LiFi maakt gebruik van lichtgolven voor datatransmissie, die niet door muren of ondoorzichtige objecten kunnen dringen. Hierdoor is het nagenoeg onmogelijk om het signaal buiten de afgeschermde ruimte te onderscheppen. De kabel die het LiFi-accesspoint in de kooi verbindt met de buitenwereld, moet worden voorzien van filters om de afscherming te waarborgen.

Meldingen en buitenbeveiliging

TEMPEST-straling lijkt op een radiosignaal, maar heeft een beperkt bereik. Buiten dit gebied vervaagt het signaal snel, net als een radio die geen ontvangst meer heeft.

Toch kunnen kwaadwillenden het signaal met geavanceerde technieken – zoals gevoelige ontvangers en richtantennes – alsnog onderscheppen. Het gebruik van richtantennes verhoogt echter het risico op ontdekking, bijvoorbeeld door een verdachte auto met antenne in de buurt van een beveiligde locatie.

Om dit te voorkomen, moet het terrein en de gebouwen rondom de beveiligde zone als één beveiligd gebied worden behandeld, vergelijkbaar met een kooi. Dit blokkeert de plaatsing van interceptieapparatuur. Maak gebruik van hekwerken, camera's, toegangspoorten en andere vormen van omtrekbeveiliging om volledige bescherming te garanderen.

Hoewel er nog geen publiek bekende incidenten zijn, wijzen verschillende signalen op hernieuwde interesse van statelijke actoren in TEMPEST. Denk aan de stijgende vraag naar interceptie-apparatuur, waargenomen busjes met antennes bij risicolocaties en de sterk toegenomen belangstelling voor TEMPEST-proof zonwering, anti-TEMPEST-folie en ander maatregelen.

Compliance en ISO 27002

TEMPEST verwijst naar een technisch fenomeen waarbij elektronische apparaten, zoals: monitoren, toetsenborden, kabels en servers, straling uitzenden die eenvoudig kan worden onderschept. In de ISO 27002-norm zijn diverse beheersmaatregelen opgenomen die betrekking hebben op interceptie. Zo richt control 7.12 Cabling security zich op het beveiligen van kabels tegen interceptie, terwijl control 8.12 Data leakage prevention eveneens interceptie adresseert. Door LiFi en TEMPEST-beveiligingsmaatregelen te implementeren, wordt voldaan aan deze ISO 27002-controls.

"Boevenvangers, de groeten…"

Referenties

https://www.nu.nl/tech/6067694/eu-legt-vier-russen-sancties-op-voor-hackaanval-op-opcw-in-den-haag.html

https://tweakers.net/nieuws/239652/politie-arresteert-17-jarigen-die-met-wifisniffer-voor-rusland-zouden-spioneren.html

https://www.signify.com/en-gb/our-company/news/press-releases/2025/20250611-signifys-trulifi-light-based-network-meets-highest-encryption-standards

https://www.hart4technology.nl/nl/tempest-beveiliging

Auteur: Chris de Vries, hoofdredacteur, en Zelfstandige Professional. Dit artikel is op persoonlijke titel geschreven.
Hij is bereikbaar via: impuls@euronet.nl

Apeldoorn-IT congres 2025

Een níet zo bekende "pareltje in de oester"

Op 20 november 2025 verwelkomde Apeldoorn meer dan 500 bezoekers op haar 10e editie van het Apeldoorn-IT congres. Schouwburg Orpheus was vanaf 08:00 tot ruim 17:15 uur het terrein voor Apeldoornse IT-professionals voor een dag: vol gesprekken, activering, ideecreatie en dus kennisdeling. Wat de locatie, de catering en de ambiance betreft een goede keuze.

In dit verslag een impressie van dit evenement. Een aanrader voor toekomstige deelname.

De structuur van dit congres

Er waren 7 thema's onderscheiden, te weten:

- **Security**
- **Artificial Intelligence**
- **Security applicatie-ontwikkeling**
- **Apeldoorn JAVA User Group (JUG)**
- **Applicatie-ontwikkeling**
- **Human aspects in IT**
- **Workshops**

Verdeeld over 4 parallelsessies en omlijst door 3 'keynotes' of in goed Nederlands "hoofdgedachte toespraken". Daarnaast een keurige en goed vallende catering. Dit alles voorafgegaan door de opening van dit jubileumcongres door burgemeester Ton Heerts.

Apeldoorns toekomst

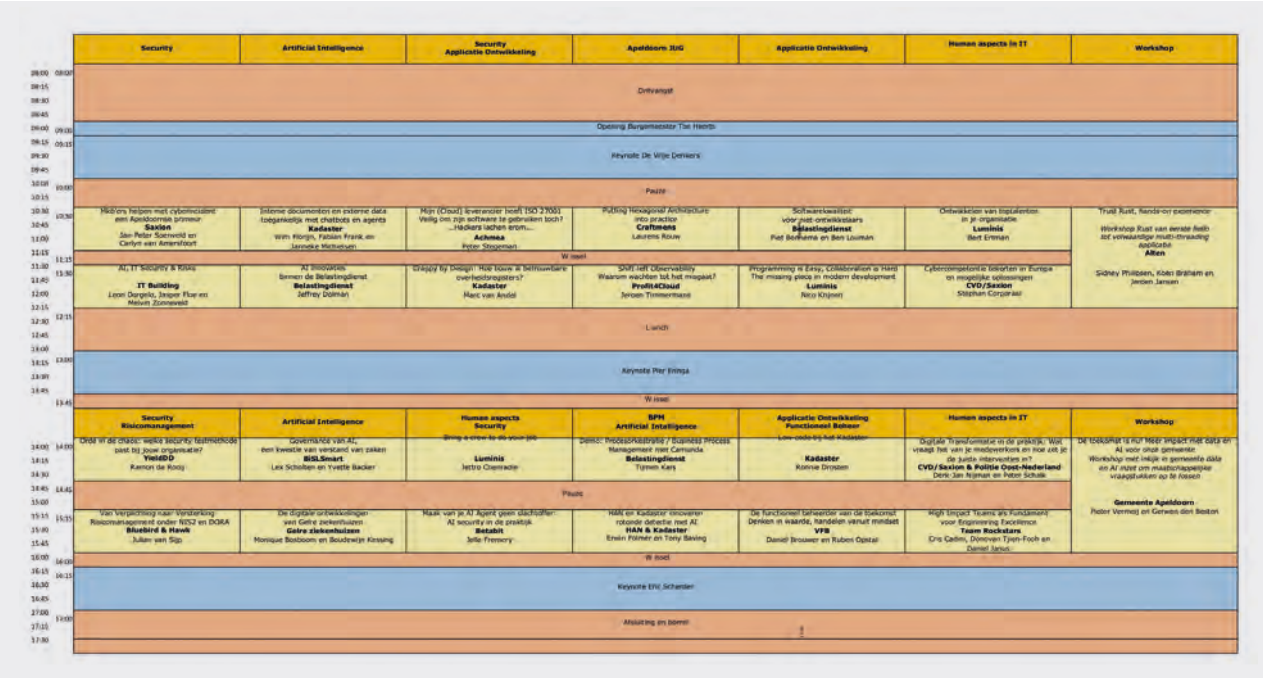
De burgemeester gaf een schets van de toekomst voor Apeldoorn en waarom IT daarin een belangrijke rol speelt. Hij gaf een beeld van een grootscheepse binnenstadrand reorganisatie. Het openbaar vervoer (busstation) zou bijvoorbeeld verplaatst worden over het spoor (d.w.z. verder weg uit het centrum), hoogbouw komt daarbij om de hoek kijken en de bestaande ontsluiting van het centrum (lees: "afsluiting") gaat wezenlijk veranderen.

Dit alles omdat Apeldoorn een stad is en wordt van grote defensie-, bedrijfs- en onderwijs-concentraties. Naast de bestaande aanwezigheid van overheidsdiensten, zoals: belastingdienst en de Nationale Politie zou dit kunnen betekenen dat de stad Apeldoorn een strategisch gewicht verkrijgt (1). Ter geruststelling de burgemeester zei dat er nog wel het nodige water door de Rijn en IJssel moeten stromen voordat dit alles gerealiseerd is/wordt.

Ton Heerts ging vervolgens nog in op de actuele risico's, zoals de discussie rondom de transfer van burgerdata naar de Verenigde Staten van Amerika (2) en de digitale accountantsverklaring, om zich te beperken tot deze.

De centrale hoofdgedachte presentatie 1

Als eerste kwamen "De Vrije Denkers" het toneel op. Zij begonnen deze dag met actie. Hun uitgangspunt was simpel: "ga over van Denken naar Doen!" Arthur Kruisman en Patrick Donath zien het als hun missie om mensen en organisaties in beweging te brengen. De door hen gepresenteerde uitgangspunten zijn zeker ook persoonlijk van aard. Aan de hand van ervaringen, met een eigen dochter, werd gezien dat tussen 5 en 8 jaar de creativiteit hoog is, zelfs het hoogst. Dan komt educatie om de hoek kijken, met zijn roosters, de structuren en kennis. Het denken wordt bevorderd op de lagere school ten kostte van een forse daling in creativiteit. Het middelbare – en hoger onderwijs, gevolgd door een beroepscarrière, geven vervolgens de genadeklap. Zij adviseren eenieder "iets te doen, onbeperkt jezelf te zijn, routine te doorbreken en meer persoonlijk leiderschap te tonen/nemen". En dus om de eigen comfort zones te doorbreken krijgt de zaal de opdracht om één buurman/vrouw aan te spreken, met die een gesprek te beginnen over wat dan ook.



Afbeelding 1: Programma Apeldoorn IT.

Afbeelding 2: de zaal in persoonlijke interactie.

Normering is het optimaal offer van menselijk potentieel

Arthur Kruisman en Patrick Donath refereerden aan Seth Godin (3) en benadrukten dat hun aanpak er een is die niet in plaats van, maar aanvullend op bestaande werkwijzen toegepast kan worden.
Na deze actieve sessie kon de 'vermoeide' zaal eerst even pauzeren en wat tot zich nemen.

Sessie 1: "Gecontroleerde innovatie" en het Kadaster

Wim Florijn en Fabian Frank presenteerden namens het Kadaster (hoofdkantoor Apeldoorn) de generieke, technische verkenning van de inzet van agents en een chatbot bij het toegankelijk maken van interne documenten en externe data. Dit ondersteunde ze met een praktische demonstratie.

Indrukwekkend was het uitgangspunt dat het Kadaster streefde naar een generiek fundament dat aan kan tonen dat innovatie en regelgeving elkaar kunnen versterken met een zorgvuldig ontworpen architectuur als randvoorwaarde. Nieuw is dat gezocht werd voorbij de grenzen van een vraag-antwoord aanpak door inzet van 'embedding', syntactisch zoeken en benutting van de **P**ublieke **D**ienstverlening **O**p de **K**aart (**PDOK**)-dataserver van het Kadaster.

Voor de complete en hoogwaardige beschrijving van deze aanpak verwijs ik naar het artikel "Gecontroleerde innovatie: de weg naar een veilige, generiek inzetbare Kadaster-chatbot" binnen deze uitgave van het magazine zie pagina 4 t/m 8.

Van non-lineair denken tot learning communities: nieuwe wegen om de cybercompetentie te vergroten.

Sessie 2: Cybercompetentie tekorten in Europa en mogelijke oplossingen

Persoonlijke interesse verleidde mij deze presentatie bij te wonen. De **N**euro**D**iverse **P**ersoon - (**NDP**) ook wel de non-lineair denkende mens genoemd, een wat vriendelijker en juistere omschrijving - ervaart een afstand tot de arbeidsmarkt. Juist hun non-lineair denkende kwaliteiten maken hen in vele gevallen geschikt voor werk in onze ICT-sector. Problemen oplossen gaat hen makkelijk af.

Organisaties echter, zijn veelal gemanaged door medewerkers/ managers die hun linkerbrein prioriteit geven alsook de hiërarchische aansturing en dus in zekere mate blind zijn voor wat de behoefte van de rechterbrein-denkenden m.b.t.: veiligheid, het gevoel en de intuïtie aan creativiteit en oplossingen te bieden hebben. Hier geldt dus m.i. dat de linker/rechterbrein discussie van het adagio moet uitgaan van: *"niet in plaats van, maar in aanvulling op!."*

Op deze plaats past het op te merken dat, vanwege ruimtegebrek in het magazine en om te voorkomen dat het een te academisch verhaal wordt, te veel nuances en details achterwege zijn gelaten in de toelichting om hier echt recht aan te doen.

Stephan Corporaal is lector Human Capital bij Saxion en houdt zich bezig met 'employability transition', dus juist ook met non-lineair denkenden mensen. Hij neemt deel aan het Europese CADMUS-project in samenwerking met het **C**entrum voor **V**eiligheid en **D**igitalisering (**CVD**). Zij richten zich op **L**even **L**ang **O**ntwikkelen (LLO), mens-tech en human capital innovaties. Hij ging in zijn toelichting in op dit project.

Europees onderzoek omvatte 606 vacatures en 249 opleidingen en trainingen, welke tot in de diepte geanalyseerd zijn. Ze analyseerden trends m.b.t. de regelgeving, technische ontwikkelingen en het risico landschap. Daarbij gingen zij van vacature analyse naar de integrale gap-analyse.

Daaruit kwamen als 5 belangrijkste discrepanties:
- Educatie en trainingsvoorzieningen.
- Personeelsontwikkeling.
- Probleemmanagement.
- Informatie Veiligheid Strategie Ontwikkeling.
- Risicomanagement.

Voor ons land zijn in 8 competenties als belangrijkste kloven terug te vinden:
- Testen.
- Probleemmanagement.
- Systeembeheer.
- Onderwijs- en opleidingsvoorzieningen.
- Personeelsontwikkelingen.
- Risicomanagement.
- Kwaliteitsmanagement en compliance.
- Informatiebeveiligingsmanagement.

De aanpak die gezocht wordt, is het creëren van 'learning communities'. Uitgangspunten: er moet een concreet probleem worden getackeld met 6 tot 10 deelnemers en 1 facilitator. Dat in samenwerking (en ten behoeve van) bedrijven en kennisinstellingen. Te investeren tijd 10-12 weken, nodig voor iteratief leren en het innoveren van werken. De houding moet zijn, dat iedere deelnemer een lerende is, dat ze samen een leergemeenschap vormen en dat men dus leert alsook experimenteert met elkaar. Centraal staat: verandering in de werkpraktijk.

Daarbij is het niet ondenkbaar dat er opeenvolgende learning communities ontstaan, mogelijk voor de verschillende fasen. Denk daarbij o.a. aan: idee-uitwerking, ontwikkeling, implementatie.

Tot slot vatte de lector Stephan Corporaal van Saxion de vraag vanuit de MKB-sector samen tot: 1. veiligheidsconsultancy; 2. applicatie- & productontwikkeling; 3. relatie-; 4. systeem- en 5. probleemmanagement.

Gezien NIS2 en de gewijzigde geo-politieke werkelijkheid is het eerste onderwerp geen verrassing. De essentie is m.i. dat het koppelen van theoretische – met de bedrijfskundige kennis voor het MKB een zeer belangrijk aandachtspunt moet zijn. Dat zal het belang van de 'learning communities' onderstrepen gekoppeld met de cybersecurityrisico's van deze tijd.

Als 'call to action' heb ik Stephan Corporaal uitgenodigd om in een volgend nummer op dit thema dieper in te gaan. Houd u ogen daarvoor open.

De centrale hoofdgedachte presentatie 2: het Gelre ziekenhuis

Na de lunch was het tijd voor een tweede keynote en wel van de heer Pier Eringa. Met zijn achtergrond bij ProRail, de grootste systeemorganisatie van Nederland, was het zijn verantwoordelijkheid daar om contracten naar de virtuele gouden medailleplak te brengen en dat pakte hij dan ook weer op voor het Gelre ziekenhuis.

De gehechtheid is vast te houden aan oude, vertrouwde systemen. Loslaten van de eigen systemen ten faveure van overkoepelende (EU-) systemen is moeilijk. Gezien de grote belangen van beide organisaties (ProRail en het Gelre ziekenhuis) was een dubbele uitvoering (redundantie, natuurlijk voor iedere organisatie voor zich langere) tijd noodzakelijk.

Zo is een belangrijke toetssteen of een systeem bij testen wel of niet blijft functioneren. Zo leidde - bijvoorbeeld bij ProRail, dat bij werk aan de Schipholtunnel met daarnaast een 'work around' werkzaamheid – tot het resultaat dat het tunnelsysteem ging flipperen tussen 2 dicht bij elkaar gelegen meetpunten en daardoor plat ging.
Het adagio in zijn vroeger en huidig werk is dan ook: 'Take risk, but manage it maximally.' en wel door activering vanuit de systeemfilters naar de top; met als doel effectiviteit en mocht dit niet bereikt worden, direct escaleren.

Sessie 3: Orde in de chaos; welke security testmethode past bij je?

Ramon de Rooij, senior security consultant bij YieldDD (4) stak van wal door de zaal voor te houden dat men moet kiezen op basis van risico, niet op basis van methode. Dat is geschraagd op hun visie dat software een echte waardecreërende factor is, mits je de software ook diepgaand begrijpt. Daar kijken ze van architectuur, beveiliging, schaalbaarheid tot en met intellectueel eigendom, onderhoudbaarheid van het systeem alsook teamcapaciteiten en nog veel meer.

In zijn presentatie nam hij de toehoorders mee via de **I**nsecure **D**irect **O**bject **R**eferences (**IDOR**), Object R (van een enkel getal tot een woord of hoog complexe structuren ten einde aan objecten waarden toe te kennen), **S**erver-**S**ide **R**equest **F**orgery (**SSRF**) en Advanced Persistent Threats; om maar enkele thema's te benoemen.

Hun taak is het ondernemingen in deze complexe zaken bij te staan (bijvoorbeeld tijdens 'due diligences' in het geval van fusies en overnames) en vaak betekent dat zij in een 'blackbox' moeten duiken. Dat is voor hen een proces van meerdere dagen; enkel het systeem te leren kennen (lees in beeld brengen) kost al vaak een dag, zo niet meer. Zo kregen de toehoorders een indruk wat er hierbij kwam kijken en werd het hun duidelijk dat tijdens de componentenontwikkeling testen al het uitgangspunt behoort te zijn Dus in mijn optiek niet alleen 'security by design', maar ook "testen als onderdeel van het ontwerpen".

Sessie 4: De functioneel beheerder van de toekomst

En zo kwamen wij alweer aan het einde van de sessies. Hier was mijn trigger dat ik meer wilde weten over de betekenis en rol van een functioneel beheerder. En dat was een goede keus, want het bleek dat deze functie wel in Nederland bestaat, maar daarbuiten vrijwel niet. Dan kan je de vraag stellen: "Zijn wij weer eens eigenwijs of juist een innovatief volkje?"

Na de presentie en kennisneming van het boek: "De functioneel beheer bundel 2 (5) neig ik te kiezen voor het laatste. Het beste toont zich dat in het "9-vlaksmodel van Rik Maes (5), zie de figuur in het artikel van Daniël Brouwer in dit magazine zie pagina 10 t/m 12, die de lezer meeneemt in zijn visie dat het denken moet uitgaan van waarde, én het handelen een groeimindset omvat (jezelf blijven ontwikkelen). Ook hier zie ik raakvlakken met de aanpak van Stephan Corporaal en de Vrije Denkers, waar ik het hiervoor al over had.

De centrale hoofdgedachte presentatie 3: “Blijf in beweging, blijf goed denken”

Erik Scherder, wie kent hem niet!? Schrijver van het boek: “Liever moe dan lui!” Als klinisch neuropsycholoog weet hij als geen ander hoe belangrijk het is te blijven denken. Met de dwarsdoorsneden van menselijke hersenen wees hij op de belangen om met nieuwe dingen bezig te zijn. Creëer je eigen hub. Blijf veel in beweging, essentieel voor een gezond leven, en dat betekent elk half uur 3 minuten uit de stoel en in beweging, zo je dat 1 keer overslaat; dan zou je bij het volgende bewegingsmoment liefst een ½ uur actief moeten zijn.

Afbeelding 3: Erik Scherder brengt ons in beweging.

Hij stelde dan ook vol overtuiging dat het huidige schoolbeleid (gericht op kinderen van lagere tot en met de middelbare school) het kind van de rekening dreigt te worden doordat onze overheid op de verkeerde aspecten bezuinigt. Zijn stelling: *“Biedt kinderen: kunst, cultuur en beweging.”*

Samenvattend:

Ik sloot voldaan en moe een dag af, die mij veel gebracht heeft en een hoofd vol impressies, gedachten en stimulansen opleverden. Ik zal mijn creativiteit aan het werk zetten. Voor jullie als gewaardeerde lezers de oproep om over 2 jaar te overwegen naar het Apeldoornse af te reizen en zelf eens te ervaren dat ook in een stad op de groene Veluwe meer te vinden is op ons vakgebied dan jullie daar wellicht zouden verwachten.

Tot over 2 jaar!

"Laat je over 2 jaar in Apeldoorn verrassen door de onverwachte mogelijkheden binnen ons vak."

Referenties

(1) Saillant detail, na de val van de Berlijnse muur en de ‘opening’ van Rusland werd bekend dat, in geval van een oorlog in West-Europa, kleine tactische Sovjet-kernbommen zouden neerdalen op Amsterdam, Zwolle en Apeldoorn. Dus wat dat betreft niets nieuws onder de zon in 2025, zie: https://www.nrc.nl/nieuws/2006/08/14/sovjet-kernbommen-op-amsterdam-zwolle-en-apeldoorn-11176713-a951927

(2) Te adviseren is de National Security Strategy 2025 of the United States of America erop na te slaan en dan met name het standpunt over de Europese Unie, zie pagina’s 25 t/m 27 Laat het duidelijk zijn dat er geen spaan heel blijft van de Europese democratie en dat er door de USA actief ingegrepen wordt om (rechts extreme) liberale ‘democratische’ en vooral nationalistische partijen aan de macht te krijgen. Zie: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

(3) Zijn eigen ‘site’: https://www.sethgodin.com/ en een Nederlandse https://www.toolshero.nl/bekende-auteurs/seth-godin/

(4) YieldDD is lid van Cyberveilig Nederland. Hun website: https://www.yielddd.com/nl/software-due-diligence/

(5) ISBN: 978.94.92790 49 1 geschreven/samengesteld door Daniël E. Brouwer, Ruben Opstal en Maurice Ummels. Zie ook: https://www.vfb.nl/9-vlaksmodel-rik-maes/ als een referentie-model voor informatiemanagement.

INFORMATIEBEVEILIGING MAGAZINE

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!

PvIB
Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Tim Deahl
Alex Dingemanse
Maarten Hartsuijker
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Fook Hwa Tan
Chris de Vries
Zoëlle Yusufi

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 2026 bedraagt € 123,- (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

Jaaroverzichten 2024 en 2025

Het was een goed gebruik om een commissie aan het werk te zetten om het beste artikel van het jaar te kiezen en de winnaar daarvan in het zonnetje te zetten. Voor 2024 en 2025 is het daarvan niet gekomen.

Wij reflecteren over hoe wij daarmee verder willen en stemmen daarmee af met het bestuur. Anderzijds willen wij graag van jullie weten wat jullie mening is/was over de artikelen van voorgaande 2 jaren.

Hiernaast een QR-code die de weg kan zijn naar elke editie van de 2 afgelopen jaren.

Scan de code en je komt uit bij een formullier waarop je kwijt kan welke artikelen jouw bijzondere aandacht/waardering hebben gehad. Graag hierbij minimaal jouw favoriete 3 artikelen opgeven.

Via dat formulier kan je dan ook doorklikken naar elk gewenste editie en artikel dat je opnieuw wenst te zien.

Wij kijken uit naar jullie respons.
Chris, Hoofdredacteur