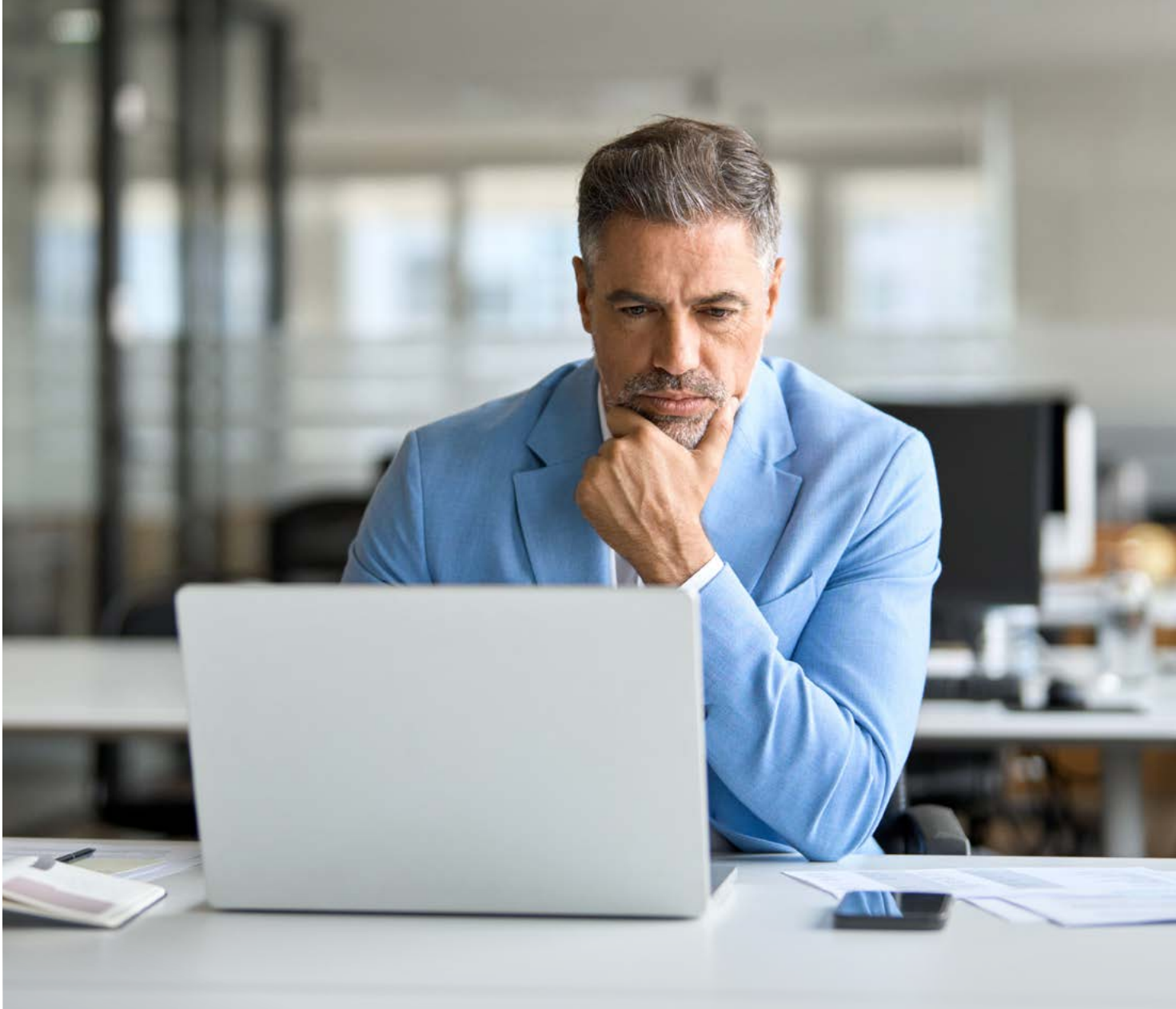


HOE GAAT U OM MET CYBER VERANTWOORDELIJKHEDEN?

Raak niet verdwaald in de cyberveiligheidsketen

Een perspectief vanuit de Managed Service Providers

Informatie

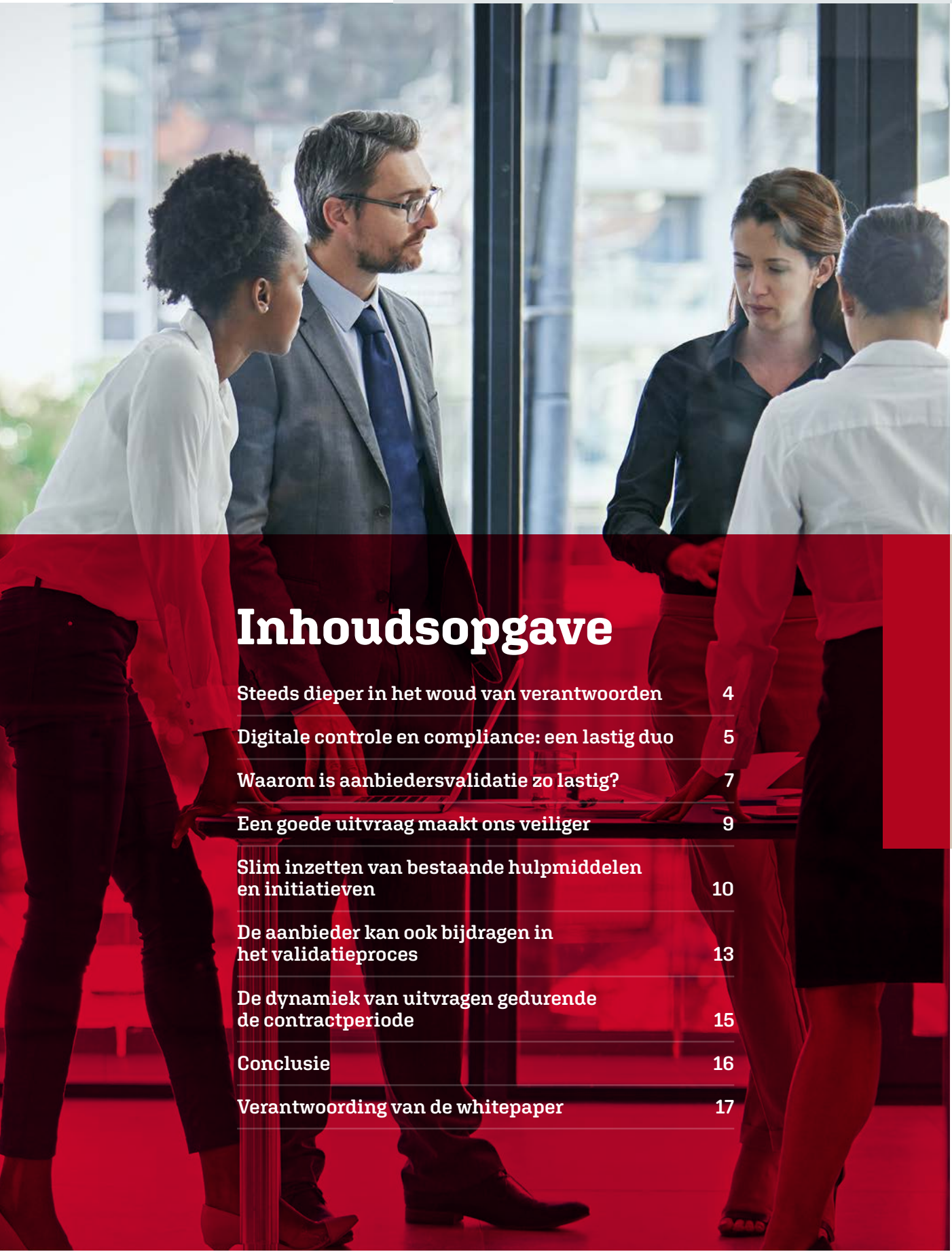
Elke organisatie is tegenwoordig wel afhankelijk van een digitale ketenpartner zoals een managed service provider, die diensten levert op het gebied van netwerk, applicatie, infrastructuur en cyberveiligheid. Op deze manier kunnen organisaties zich focussen op hun kernactiviteiten en worden zij ondersteund door partners met digitale diensten. Deze digitale afhankelijkheid brengt echter ook risico's met zich mee. Zijn deze risico's goed beheersbaar? Dat is de vraag die klanten, auditors en toezichthouders bezighoudt. Maar hoe kun je dat aantonen?

Deze whitepaper beschrijft de uitdagingen en kansen waarmee organisaties worden geconfronteerd in hun zoektocht naar een effectieve aanpak om ketenrisico's aantoonbaar te beheersen. De inzichten in dit whitepaper bieden handvatten om samen duidelijke afspraken te maken.

De auteurs
Kelvin Rorive (CISO - ICT Group)
Wijnand Goedhart (CISO - Esprit ICT)
Roel Gloudemans (CSO - Conclusion)
Merik Spitteler (Cybersecurity Lead - Verschillende organisaties)
Frank Breedijk (CISO – Schuberg Philis)
Maarten Leeuwerik (Security Business Partner - CGI)
Sammy Rhuggernaath (Manager Security Governance - DXC.technologies)
Jack Krul (CISO – Exact)

Deze whitepaper is een uitgave van het MSP-ISAC (Managed Service Provider – Information Sharing & Analysis Centre) waarin de volgende organisaties zijn vertegenwoordigd: Atos, Capgemini, Cegeka, Centric, CGI, Conclusion, DXC, Esprit ICT, Exact, ICT Group, Odin-groep, SchubergPhilis, Sogeti, Solvinity, NCSC, Poliitie en wordt gesponsored door stichting CCRC (Cyber Chain Resilience Consortium)

Cyber Chain Resilience Consortium



Inhoudsopgave

Steeds dieper in het woud van verantwoorden

Aanleiding voor het onderzoek

In een wereld waarin organisaties steeds sterker verbonden zijn via digitale tools, is de impact van beveiligingsproblemen voelbaar in de hele keten. Deze whitepaper gaat in op de cruciale vraag hoe bedrijven effectief kunnen omgaan met de beveiligingsrisico's die ontstaan door deze onderlinge afhankelijkheid. Het traditionele gebruik van SOC (System and Organization Controls) verklaringen, ISAE3000, ISO27001-certificeringen, en eigen vragenlijsten vormen vaak een basis voor afnemers om de cyberveiligheid bij hun aanbieders te toetsen. Deze aanpak brengt ook de uitdaging met zich mee dat het beantwoorden van al deze vragenlijsten voor de aanbieder steeds tijdsintensiever wordt. Met de komst van nieuwe wetgeving, zoals NIS2 en DORA, wordt verwacht dat deze druk alleen maar zal toenemen. Dit roept de vraag op of deze methoden wel optimaal zijn, en zo ja, hoe ze slimmer en efficiënter kunnen worden ingezet.

Deze paper beschrijft praktische tips voor zowel leveranciers als afnemers om digitale beveiligingsrisico's in een steeds meer onderling verbonden wereld effectief te beheren.

De doelgroepen van deze paper zijn CISO's, CIO's, en afdelingen voor Risk & Compliance en inkoop. Hoewel er veel meer aspecten van belang zijn bij het beheersen van risico's in toeleveringsketens, ligt de focus in deze whitepaper op informatiebeveiliging, cyberveiligheid en privacy.

In deze paper wordt de onderstaande terminologie gehanteerd:

- **Uitvraag**: Beschrijft een verzoek aan de leverancier als waarborg dat een bestaande dienst of product (nog) voldoet aan de eisen van de afnemer.
- **Afnemer**: Elke zakelijke organisatie die een dienst of product afneemt van een leverancier, de aanbieder.
- **Aanbieder**: Een organisatie die een bepaalde dienst of product levert die voldoet aan bepaalde eisen.
- **Ketenpartner**: Een afnemer of aanbieder die digitaal afhankelijk is van een andere organisatie en/of aanbieder.

Digitale controle en compliance: een lastig duo

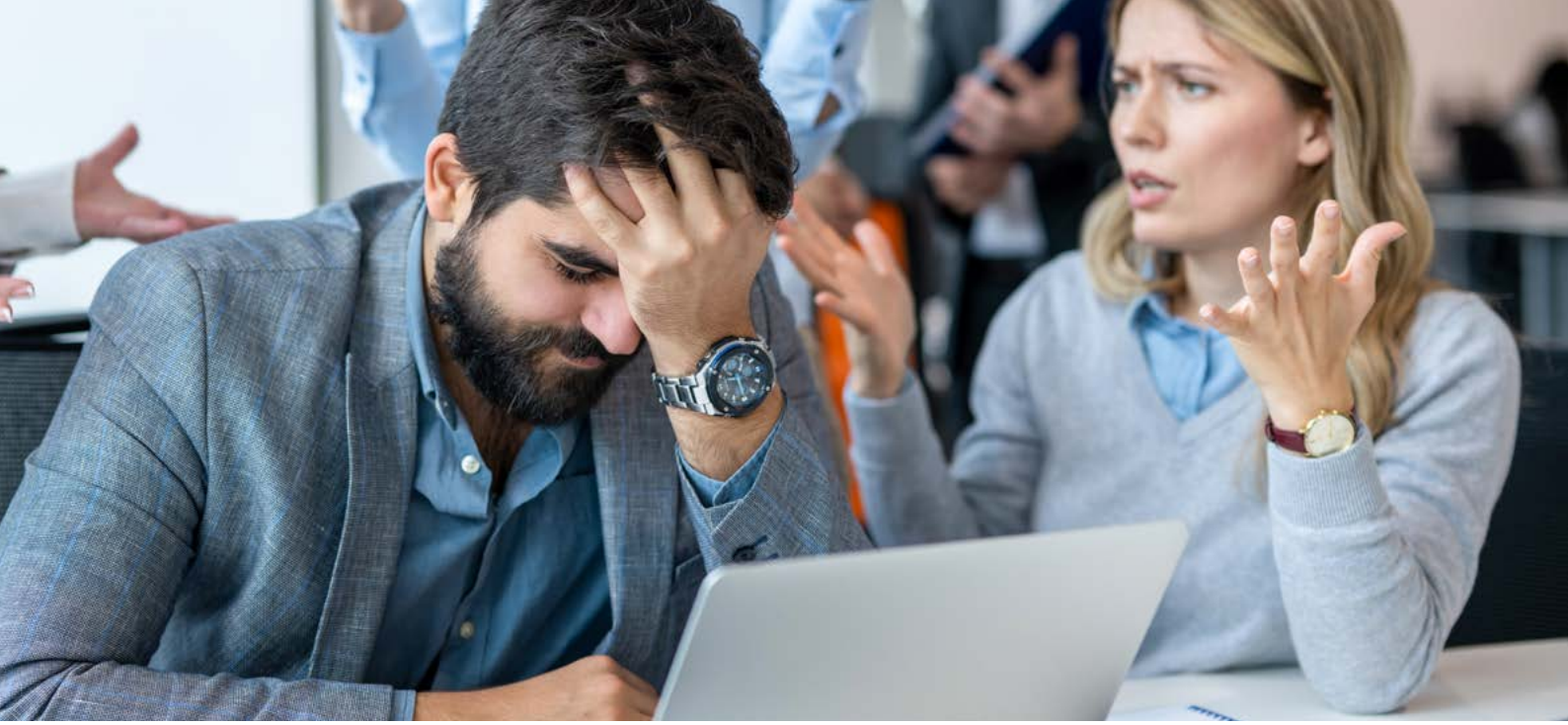
Het belang van digitale controle over je ketenpartners, zowel richting afnemers als aanbieders, neemt toe. Dit wordt ook erkend door onze toezichthouders en wetgevers. Zij ontwikkelen normenkaders en wetten (DSA, CRA, NIS2, DORA) die niet alleen bijdragen aan een betere cyberveiligheid binnen individuele organisaties, maar ook de samenhang binnen de hele keten versterken. Het gevolg is dat we willen, en in veel gevallen moeten, voldoen aan deze normenkaders en wetten.

Het vraagt om specifieke expertise om deze normenkaders goed te implementeren. En dat is vaak waar het misgaat. Afnemende organisaties beschikken vaak niet over de benodigde kennis. Maar wat is de impact daarvan?

Digitale controle in de keten voor afnemers en aanbieders is niet vanzelfsprekend

Er zijn verschillende redenen waarom de gemiddelde organisatie moeite heeft met het krijgen van digitale controle over de keten:

- **Complexiteit van de eigen organisatie en dienstverlening:** Vaak ontbreekt het aan inzicht in de risico's binnen de bedrijfsprocessen, waardoor het moeilijk is om ketenpartners effectief te integreren en de juiste verantwoordelijkheden toe te wijzen.
- **Complexiteit van beveiligingstechnologieën:** Informatiebeveiliging is een breed en complex domein dat expertise vereist. Zonder een duidelijke visie en strategie op gebied van cyberweerbaarheid, is het moeilijk om ketenpartners optimaal in te zetten.
- **Snel veranderende bedreigingslandschap:** Cyberveiligheid bedreigingen evolueren continu, waardoor strategieën en aanpak voortdurend moeten worden aangepast. Het risico om achter te blijven bij het afstemmen van controls met ketenpartners om de cyberweerbaarheid in de keten te waarborgen, is reëel.
- **Diepgaande kennis van compliance-vereisten:** Verschillende sectoren hebben verschillende compliance-eisen die gespecialiseerde kennis vereisen. Zo kennen we bijvoorbeeld voor de financiële sector heel specifiek de DORA en voor de zorg de NEN7510. Zonder een goed beeld bij deze eisen, bestaat het risico dat ketenpartners onvoldoende bijdragen aan het naleven ervan.
- **Risicobeoordeling:** Om voldoende cyberweerbaar te zijn, is het cruciaal om te weten waar de grootste risico's liggen, wat een gedegen risicoanalyse vereist. Dit vraagt om specialistische kennis. Als niet duidelijk is waar de risico's zich bevinden, loop je het risico de zwakste schakel in de keten te zijn.
- **Traditioneel perspectief:** Veel organisaties hebben van oudsher weinig aandacht besteed aan beveiliging en privacy waardoor er een aanzienlijke achterstand is ontstaan en de (keten) kwetsbaarheid is toegenomen.



- **Toenemende regeldruk:** onevenredig grote last voor organisaties
  Wetgeving zoals DORA en de Cyberbeveiligingswet (NIS2), evenals normen als ISO27001 en IEC 62443, stellen organisaties voor de uitdaging om strenge beveiligingsmaatregelen te implementeren, wat veel inspanning vergt. Het wordt steeds gebruikelijker dat bedrijven moeten aantonen dat hun ketenpartners cyberweerbaar zijn. Door deze toenemende en snel veranderende regelgeving ervaren veel organisaties dit als een disproportionele last.

Afnemers beschouwen 'non-conformiteit' dan ook steeds vaker als het grootste risico, vooral vanwege de hoge boetes die toezichthouders kunnen opleggen. Enkele banken zijn al bestraft met miljoenenboetes voor het niet naleven van de regelgeving.

Risico! Creatieve aanbiedersvalidatie

Bij het verkrijgen van digitale controle over de keten speelt de inkoper of contractbeheerder van de afnemende organisatie een cruciale rol. Zij zijn verantwoordelijk voor het sluiten van overeenkomsten die ervoor zorgen dat aanbieders aan de beveiligingseisen voldoen. Daarnaast moeten ze periodiek bestaande contracten herzien om te verifiëren dat deze nog steeds in lijn zijn met de geldende regelgeving. Dit is vooral belangrijk gezien de voortdurend veranderende en aangescherpte regelgeving op het gebied van cyberveiligheid.

Een inkoopproces begint altijd met een behoefte uit de markt. In het ideale geval wordt bij het formuleren van deze behoeften steun gezocht bij materiedeskundigen binnen de eigen organisatie. Wanneer deze kennis ontbreekt, worden er creatieve oplossingen ingezet. Dit kan uiteenlopen van het opnieuw gebruiken van checklists uit eerdere projecten tot het inschakelen van generatieve kunstmatige intelligentie om gedetailleerde en ogenschijnlijk goed doordachte verzoeken te creëren. Dit resulteert echter vaak in een algemene vraagstelling die essentiële details mist met twee nadelen als gevolg: 1) de klant ontvangt niet de beste oplossing en 2) de leverancier besteedt onnodig veel tijd aan een verzoek vol inconsistenties, waardoor de klant mogelijk niet de offerte ontvangt die hij werkelijk nodig heeft.

Bovendien kan deze aanpak ertoe leiden dat aanbieders veel tijd kwijt zijn aan het beantwoorden van ineffectieve vragenlijsten, ten koste van de tijd die ze kunnen besteden aan het versterken van de cyberweerbaarheid. Vaak zijn het namelijk juist de specialisten die worden ingeschakeld om deze vragenlijsten in te vullen.

Waarom is aanbieders-validatie zo lastig?

Door de diversiteit aan relevante factoren is het voor veel afnemende organisaties een uitdaging om tijdens inkooptrajecten of herbeoordelingen binnen contractperiodes een effectieve validatie van aanbieders uit te voeren.

Dit hoofdstuk belicht de complexiteit en mogelijke valkuilen bij het behouden van controle over partijen binnen de keten.

De complexiteit van normen en certificeringen

Voor afnemende organisaties is het vaak een voordeel als de aanbiedende organisatie beschikt over certificeringen op het gebied van informatiebeveiliging, zoals ISO 27001, NIST, SOC2, en ISAE3402. Elke norm heeft echter zijn eigen terminologie en vereisten, wat het begrip en de samenhang bemoeilijkt. Want, welke certificering moet een afnemende organisatie dan verlangen van de aanbieder?

Daarnaast zijn er ook wetgevingen waar de aanbieders aan moeten voldoen, zoals GDPR (voor privacy), PCI-DSS (voor kaartbetalingsbeveiliging) en de recente Cyberbeveiligingswet (op basis van de NIS2 - Network and Information Security2). Moeten organisaties die onder deze wetten vallen nog aanvullende certificeringen hebben? Voor de afnemende organisatie is het ingewikkeld om wegwijs te worden in dit landschap van certificeringen en wetten.

Voor de afnemer is het vaak lastig om te bepalen of aanvullende validatie nodig is bij een aanbieder die beschikt over een bepaalde certificering op het gebied van informatiebeveiliging.
Een voorbeeld ter illustratie: het stellen van een vraag over de status van de databack-up van een aanbieder kan overbodig zijn als er al een SOC-assurance rapport beschikbaar is, waarin de back-up procedures in de toepassingsverklaring zijn opgenomen. Een meer relevante validatievraag zou kunnen gaan over de aanwezigheid van medewerkers van de aanbieder in Nederland.

Met de juiste expertise is dit prima te beoordelen, maar die is lang niet altijd aanwezig bij afnemende organisaties.

Cyberveiligheid is niet one-size-fits-all

Elke onderneming krijgt te maken met unieke cyberdreigingen. Zo loopt een dienstverlener in een kritieke sector, zoals energievoorziening of watermanagement, andere risico's dan een bedrijf dat promotionele artikelen verkoopt. Afnemers moeten strengere beveiligingseisen stellen aan leveranciers die een substantiële invloed hebben op hun bedrijfsprocessen, in vergelijking met leveranciers die slechts een marginale invloed hebben.

Het principe "Security is niet one-size-fits-all" bemoeilijkt het proces van aanbiedersvalidatie, omdat afnemers moeten bepalen welk beveiligingsniveau passend is voor hun specifieke behoeften. Een grondige risicoanalyse is hierbij van grote waarde. Dit helpt de afnemer om de werkelijke behoeften en risico´s te begrijpen en om op maat gemaakte beveiligingseisen op te stellen die aansluiten bij de aanbieder. Een mooi voorbeeld hiervan is het vragen om een 24/7 dienstverlening van een leverancier terwijl de afnemer zelf slechts 5x10 uur beschikbaar is.
Er bestaat dus geen one-size-fits-all aanpak voor aanbiedersvalidatie. Het uitvoeren van een dergelijke analyse vereist expertise, die niet in elke organisatie aanwezig is.

Het gaat om de specifieke vragen

De voorgaande paragrafen maken duidelijk dat het opstellen van een nauwkeurige en relevante uitvraag geen gemakkelijke taak is. De complexiteit van de normen en de kosten van expertise maken het uitvraagproces zeer uitdagend, waardoor de neiging om te vertrouwen op uitgebreide, gestandaardiseerde vragenlijsten begrijpelijk, maar niet effectief. Dit benadrukt de uitdagingen waar afnemers mee te maken hebben bij het streven naar een waardevolle validatie van aanbieders.

In het volgende deel bespreken we de voordelen van een goed opgestelde uitvraag voor alle betrokken partijen.

Een goede uitvraag maakt ons veiliger

Het verfijnen van de aanbiedersvalidatie biedt aanzienlijke voordelen voor de cyberweerbaarheid in de keten evenals voor de kosten en effectiviteit van het validatieproces, zowel voor aanbieders als afnemers. Een duidelijke en specifieke vragenlijst zorgt ervoor dat de aanbieder minder interne kosten maakt voor het beantwoorden en beheren van uitvragen. Deze efficiëntie kan leiden tot lagere operationele kosten, wat uiteindelijk resulteert in een gunstigere prijs voor de afnemer.

Dit effect versterkt zichzelf door de keten heen. Elke schakel, van partij A tot B en van B tot C, kan te maken krijgen met een cascade van uitvragen. Deze opeenstapeling van vragenlijsten leidt tot aanzienlijke kosten voor de hele keten. Door slim en gericht uit te vragen, kan deze piramide van validatie veel efficiënter worden uitgevoerd, wat resulteert in significante kostenbesparingen voor alle betrokken partijen.

Een goede aanbiedersvalidatie is een krachtig instrument dat niet alleen de behoeften van de afnemer in kaart brengt, maar ook de aanbieder de kans geeft zijn expertise optimaal te tonen. Door een duidelijk en weloverwogen beeld te schetsen van de specifieke vereisten, kan de aanbieder niet alleen adequaat op de uitvraag reageren, maar ook proactief waar nodig aanvullen. Dit resulteert in een aanbod dat zowel technisch als strategisch aansluit bij de vraag en de cyberweerbaarheid van de afnemer vergroot. Bovendien leidt deze nauwkeurige afstemming tot lagere kosten, doordat de dienstverlening beter is afgestemd op de werkelijke behoeften. Dit synergetische effect tussen aanbieder en afnemer versterkt zowel de algehele cyberveiligheid als de efficiëntie binnen de keten.

Het is duidelijk dat een goede aanbiedersvalidatie voordelen biedt voor alle partijen in de keten, tot aan de consument, die profiteert van lagere prijzen doordat er minder kosten worden gemaakt in het validatieproces. Maar hoe bereiken we zo'n effectieve aanbiedersvalidatie?

Slim inzetten van bestaande hulpmiddelen en initiatieven

In een ideale situatie heeft een afnemer voldoende expertise om een kwalitatief goede aanbiedersvalidatie te doen. Maar, vaak ontbreekt die expertise, terwijl de afnemer wel digitale controle over de aanbieder wil behouden. Gelukkig zijn er verschillende hulpmiddelen en initiatieven beschikbaar waarmee afnemers, ook zonder specialistische kennis, een degelijke validate kunnen uitvoeren.

Hieronder volgt een overzicht van enkele van deze hulpmiddelen en initiatieven.

Eenduidigheid in terminologie

Misverstanden ontstaan vaak door miscommunicatie, vooral wanneer de terminologie niet goed is afgestemd. Dit risico bestaat ook tussen aanbieder en afnemer. Het gebruik van eenduidige terminologie kan het validatieproces aanzienlijk verbeteren. Cyberveilig Nederland heeft hiervoor het Cyber Security Woordenboek uitgebracht (zie kader). Door dit toe te passen, zorgen alle partijen ervoor dat zij dezelfde definities en concepten hanteren.

De Online Trust Coalitie (OTC)

Het Cyber Security Woordenboek van Cyberveilig Nederland is een waardevolle bron voor iedereen die betrokken is bij cyberveiligheid. Het biedt gestandaardiseerde definities en terminologie, wat essentieel is voor heldere communicatie binnen het veld. Hier is het woordenboek te downloaden: https://www.cyberveilignederland.nl/download/file/CybersecurityWoordenboek2021.pdf

Vereenvoudigde risicoanalyse

Risicoanalyses in de context van informatiebeveiliging zijn complex, omdat ze verschillende dimensies omvatten. Ze vereisen inzicht in technologische aspecten, kennis van organisatorische processen en goed begrip van het voortdurend veranderende bedreigingslandschap. Dit vraagt om diepgaande expertise om de waarschijnlijkheid en impact van potentiële risico's nauwkeurig te beoordelen. Dit maakt aanbiedersvalidatie lastig, omdat het niet altijd duidelijk is waar de nadruk op moet liggen bij cyberweerbaarheid.

Het Digital Trust Center van het Ministerie van Economische Zaken ondersteunt ondernemend Nederland op het gebied van cybersecurity. Zij hebben een vereenvoudigede risicoanalyse ontwikkeld waarmee organisaties met 9 eenvoudige vragen kunnen vaststellen welke risicoklasse van toepassing is.
Zie daarvoor https://www.digitaltrustcenter.nl/risicoklasse

Met deze inzichten kunnen organisaties beter bepalen welke beveiligingsmaatregelen nodig zijn voor de afnemer en dus beter aangeven welke maatregelen met welke kwaliteitseisen worden verwacht bij een aanbieder. Bijvoorbeeld: als de aanbieder met persoonsgegevens of vertrouwelijke informatie werkt, zijn strengere beveiligings-maatregelen vereist dan wanneer er alleen met publieke informatie wordt gewerkt.

Bestaande initiatieven

Verschillende initiatieven streven ernaar om de betrouwbaarheid van aanbieders van IT-producten en -diensten, zoals clouddiensten, te beoordelen, elk vanuit een eigen perspectief.

De Online Trust Coalitie (OTC) focust op het veilig gebruik van clouddiensten. Deze coalitie biedt diverse hulpmiddelen aan om de keuze voor een betrouwbare cloudprovider makkelijker te maken. Geïnteresseerden in clouddiensten worden aangeraden als eerste stap de beschikbare tools van de OTC te raadplegen (zie kader).

Een ander initiatief, het Cyberkeurmerk, is opgezet om het selecteren van aanbieders te verfijnen. Dit keurmerk helpt ondernemers te beoordelen of aanbieders voldoende beveiligingsmaatregelen treffen. Eind 2023 gaf de Tweede Kamer groen licht voor de ontwikkeling van dit keurmerk specifiek gericht op MKB-aanbieders. Met de steun van het Digital Trust Center, brancheorganisaties en het Centrum voor Criminaliteitspreventie en Veiligheid (CCV)[1], een onafhankelijke stichting, biedt dit keurmerk kleine ondernemers een hulpmiddel om IT-diensten voor cyberveiligheid te kiezen. Het CCV, bekend om het ontwikkelen van keurmerken en certificaten die de kwaliteit van IT-producten en -diensten waarborgen, is verantwoordelijk voor de realisatie van dit nieuwe cyberkeurmerk.

Tot slot is er CYRA (CYberRAting)[2], een initiatief dat het selecteren van aanbieders vereenvoudigt. Leveranciers met een CYRA-certificering garanderen een vastgesteld niveau van betrouwbaarheid en kwaliteit op het gebied van cyberveiligheid. Dit certificeringstraject helpt afnemers om gericht en specifiek aanbieders te selecteren. CYRA bevordert digitale weerbaarheid door ondernemers een zelfevaluatie- en certificeringstraject aan te bieden. Dit groeimodel leidt bedrijven van een basisniveau in digitale veiligheid naar geavanceerde normen, zoals ISO 27001. Het initiatief, ontwikkeld in samenwerking met verschillende partners, maakt digitale weerbaarheid toegankelijker en ondersteunt bedrijven bij het naleven van relevante wetgeving, zoals de GDPR en NIS2.

Inzet van Security Rating Diensten

Security Rating Diensten, ook wel scoringsbedrijven genoemd, winnen snel aan populariteit in de wereld van cyberveiligheid. Deze diensten beoordelen de cyberveiligheid prestaties van organisaties op basis van openbare informatie en geven een score die kan helpen bij de aanbiedersvalidatie.

Het is echter belangrijk te beseffen dat deze scores niet de absolute waarheid zijn, maar eerder een indicatie van de beveiligingsstatus. Ze dienen als startpunt voor gesprekken over beveiliging en zouden niet als doorslaggevend criterium moeten worden gebruikt bij de keuze van een aanbieder.

[1] https://hetccv.nl/minister-wil-cybersecurity-keurmerk-om-mkb-te-helpen
[2] https://cyberrating.nl/over-ons

De Online Trust Coalitie (OTC)[1]

Deze biedt strategische voordelen voor organisaties die slim clouddiensten willen inkopen. Het initiatief, gesteund door overheid, bedrijfsleven en wetenschap, zet zich in voor betrouwbare clouddiensten door het bevorderen van transparantie en standaardisatie.

Voordelen van de OTC bij het inkopen van clouddiensten zijn:

1. De OTC stimuleert uniforme, gestandaardiseerde benaderingen, waardoor organisaties gemakkelijker de betrouwbaarheid van clouddiensten kunnen beoordelen.
2. Door publiek-private samenwerking werkt de OTC aan het opbouwen van vertrouwen in de cloud, cruciaal voor veilige en efficiënte digitale transacties.
3. Met de focus op heldere criteria, controlemechanismen en communicatiestandaarden, maakt de OTC het eenvoudiger voor organisaties om de cyberveiligheid en conformiteit van clouddiensten te verifiëren.

De OTC levert een fundamentele bijdrage aan het versterken van de digitale infrastructuur, door helderheid en vertrouwen te bieden in de complexe wereld van clouddiensten. Dit is essentieel voor organisaties die streven naar een veilige, betrouwbare en efficiënte inzet van cloud technologieën.

[1] https://onlinetrustcoalitie.nl/

Voor afnemers met veel aanbieders bieden deze diensten een efficiënte manier om de beveiligingsstatus van verschillende partijen te beoordelen. Bij organisaties met minder aanbieders kan het voordeliger zijn gebruik te maken van adviesbureaus die een abonnement hebben bij een Security Rating organisatie, wat de kosten van een eigen abonnement bespaard.

Security Rating Diensten dragen bij aan een volwassen gesprek over beveiliging tussen afnemers en aanbieders en stimuleren continue verbetering en bewustzijn van cyberveiligheid. Bekende aanbieders van deze diensten zijn BitSight, SecurityScorecard, UpGuard, RiskRecon, en Panorays.

Kortom, Security Rating Diensten zijn waardevol in het proces van aanbiedersvalidatie.

De aanbieder kan ook bijdragen in het validatieproces

Openheid over beveiligingsaanpak aanbieders

Openheid van aanbieders over hun beveiligingsaanpak kan de kwaliteit van een uitvraag aanzienlijk verhogen. Wanneer aanbieders transparant zijn over hun benadering van cyberveiligheid, de normen die zij hanteren en hoe zij beveiliging op verschillende niveaus waarborgen, kunnen afnemers gerichter en relevanter vragen stellen tijdens het validatieproces. Zo kan een aanbieder, door de verklaring van toepasselijkheid van het ISO27001-certificaat te delen, de afnemer in staat stellen om specifieke vragen te stellen over de implementatiedetails. Dit leidt tot een beter begrip van de beveiligingsmaatregelen van de aanbieder. Zie het onderstaande kader voor meer redenen om transparant te zijn over de cyberveiligheidsaanpak.

Een open uitnodiging tot vertrouwen en samenwerking

In een tijdperk waarin cyberveiligheid onlosmakelijk verbonden is met het succes van een organisatie, is transparantie niet langer een luxe, maar een noodzaak. Het openbaar maken van uw informatiebeveiligingsaanpak en -beleid op bijvoorbeeld uw website is een krachtige stap die vertrouwen schept, samenwerking bevordert en uw organisatie positioneert als een verantwoordelijke en betrouwbare partner in de digitale wereld. Een aantal redenen om deze aanpak in overweging te nemen:

1. Bouwen aan vertrouwen

Klanten, partners en stakeholders willen samenwerken met organisaties die ze kunnen vertrouwen. Door uw beveiligingsbeleid en -aanpak openbaar te maken, geeft u een duidelijk signaal af dat u transparantie en cyberveiligheid serieus neemt. Dit bouwt niet alleen vertrouwen op, maar versterkt ook uw reputatie als een cyberveiligheidsbewuste organisatie.

2. Voldoen aan regelgeving

Veel industrieën hebben strikte regelgeving wat betreft informatiebeveiliging en privacy. Door uw beleid openbaar te maken, laat u zien dat uw organisatie niet alleen voldoet aan deze regels, maar ook bereid is om uw aanpak proactief te delen met toezichthouders en het publiek.

3. Aantrekken en behouden van talent

Professionals in de IT en beveiliging zijn vaak op zoek naar organisaties die een duidelijke en serieuze benadering van beveiliging hanteren. Een transparante informatiebeveiligingsaanpak kan toptalent aantrekken en behouden.

4. Bevorderen van klantbetrokkenheid

Klanten waarderen wanneer organisaties open zijn over hoe ze gegevens beschermen. Dit kan de klantbetrokkenheid verhogen en de klanttevredenheid verbeteren, omdat klanten zich meer betrokken en veiliger voelen.

5. Verbeteren van interne processen

Het proces van het openbaar maken van uw informatiebeveiligingsbeleid dwingt tot interne evaluatie en afstemming. Dit kan leiden tot verbeteringen in uw beveiligingsprotocollen en bedrijfsprocessen, wat resulteert in een sterkere beveiligingshouding.

6. Samenwerking en gemeenschapsopbouw

Door uw beveiligingspraktijken open te delen, nodigt u feedback en samenwerking uit van andere organisaties, experts en belanghebbenden. Dit kan leiden tot betere beveiligingspraktijken en sterkere relaties binnen uw industrie.

Zorgplicht van aanbieders

De zorgplicht van aanbieders is een juridisch principe dat voortkomt uit artikel 7:401 van het Nederlandse Burgerlijk Wetboek. Dit artikel stelt dat een aanbieder bij het uitvoeren van de opdracht de zorg van een goed opdrachtnemer in acht moet nemen. In het onderstaande kader wordt een zaak beschreven: Een IT-specialist is op grond van de zorgplicht niet alleen verantwoordelijk voor het opzetten en onderhouden van de IT-infrastructuur, maar moet dit ook doen met de nodige professionaliteit en zorgvuldigheid, in overeenstemming met de geldende technische normen en richtlijnen, vooral op het gebied van beveiliging.

Zaaknummer C/13/640668 / HA ZA 17-1380

In deze zaak heeft een afnemer een IT-specialist aangeklaagd vanwege onvoldoende beveiliging van de IT-infrastructuur. De afnemer werd slachtoffer van een ransomware-aanval en moest betalen om toegang tot de bestanden terug te krijgen. Een onderzoek wees uit dat betere netwerkbeveiliging en back-upvoorzieningen de aanval hadden kunnen voorkomen.

De afnemer eiste een schadevergoeding met de bewering dat de IT-specialist zijn opdracht en zorgplicht niet naar behoren had vervuld. De IT-specialist verweerde zich door aan te geven dat de afnemer bepaalde beveiligingsmaatregelen had afgewezen.

De rechtbank oordeelde dat de IT-specialist tekort was geschoten, vooral in het bieden van adequate beveiliging. Echter, de afnemer werd ook verantwoordelijk gehouden, met name voor het gebruik van zwakke wachtwoorden. De schade werd verdeeld, waarbij 2/3 aan de IT-specialist werd toegeschreven. De IT-specialist werd ook veroordeeld tot het betalen van de proceskosten in deze tegeneis.

In deze zaak oordeelde de rechtbank dat de IT-specialist zijn zorgplicht had geschonden door geen adequate beveiligingsmaatregelen te implementeren en door te falen in het bieden van een betrouwbaar back-upsysteem, waardoor de afnemer kwetsbaar was voor de ransomware-aanval. Het feit dat de afnemer sommige beveiligingsmaatregelen had afgewezen, ontsloeg de IT-specialist niet van zijn verantwoordelijkheid om te adviseren en te waarschuwen voor de risico's.

Een aanbieder moet dus ook hier zijn verantwoordelijkheid nemen, al tijdens de uitvraag bij de initiële selectie. Als een afnemer niet bereid is beveiliging af te nemen die wel belangrijk wordt geacht door de aanbieder, dan zou de aanbieder geen aanbieding moeten doen. Dit gezien de afbreukrisico's voor beide partijen.

De dynamiek van uitvragen gedurende de contractperiode

Een dynamische aanbiedersvalidatie biedt ook een structureel kader voor verantwoording, zowel intern als naar externe toezichthouders. Het documenteert hoe veranderingen worden beheerd, besluiten worden genomen en hoe de dienstverlening blijft voldoen aan de geldende normen en regelgeving. Ook in de recente Cyberbeveiligingswet (NIS2) is de continue aanbiedersevaluatie van aanbieders een belangrijk onderwerp om cybersecurityrisico's in de gehele keten te mitigeren.

De aanbiedersvalidatie als continu proces

Hoewel de initiële selectie van een aanbieder een belangrijke stap is, houdt de relevantie van de aanbiedersvalidatie daar niet op. De markt, technologieën en bedrijfsbehoeften veranderen voortdurend, waardoor een aanvankelijk optimale keuze snel kan verouderen (zie kader). Daarom is het essentieel om de aanbiedersvalidatie als een continu proces te beschouwen, waarbij regelmatige evaluatie en communicatie tussen afnemer en aanbieder centraal staan.

Tijdens de contractperiode zorgt een voortdurende dialoog, ingebed in de aanbiedersvalidatie, ervoor dat zowel afnemer als aanbieder alert blijven. Deze interactie is essentieel om te waarborgen dat de geleverde diensten of producten blijven voldoen aan de veranderende behoeften van de afnemer en aan de evoluerende marktstandaarden.

Een dynamische aanbiedersvalidatie biedt ook een structureel kader voor verantwoording, zowel intern als naar externe toezichthouders. Het documenteert hoe veranderingen worden beheerd, besluiten worden genomen en hoe de dienstverlening blijft voldoen aan de geldende normen en regelgeving. Ook in de recente Cyberbeveiligingswet (NIS2) is de continue aanbiedersevaluatie van aanbieders een belangrijk onderwerp om cybersecurityrisico's in de gehele keten te mitigeren.

Voorbeelden van veranderingen die kunnen optreden tijdens een contractperiode zijn:

- **Nieuwe veiligheidsdreigingen**: Nieuwe soorten aanvallen kunnen bestaande verdedigingsmechanismen verouderd maken, wat een snelle reactie vereist.
- **Veranderende organisaties:** Doel van een organisatie kan verschuiven en dat leidt weer tot veranderende eisen aan de dienstverlening.
- **Regelgevende wijzigingen:** Op het gebied van cyberweerbaarheid verandert de wetgeving snel.
- **Technologische vooruitgang:** De snelle ontwikkeling van technologieën zoals AI en machine learning kan invloed hebben op de beveiligingsmechanismen.

Conclusie

Aanbieders merken een toename in het aantal vragenlijsten die worden verstuurd om de betrouwbaarheid op het gebied van cyberveiligheid te toetsen. Dit zorgt voor een aanzienlijke werklast voor zowel aanbieders als afnemers, wat de effectiviteit van deze aanpak ter discussie stelt. Deze whitepaper beschrijft de oorzaken en onderzoekt mogelijke verbeteringen.

Een belangrijke oorzaak lijkt het gebrek aan expertise bij afnemers in het proces van aanbiedersvalidatie. Door dit gebrek aan kennis wenden afnemers zich vaak tot creatieve oplossingen zoals het kopiëren of genereren van vragenlijsten met behulp van Generatieve Artificial Intelligence (AI). Hierbij wordt het eigenlijke doel van de validatie - het waarborgen van de cyberweerbaarheid in samenwerking met partners – vaak uit het oog verloren. Dit is onhoudbaar, zeker nu regelgeving steeds strenger wordt en nog meer vragenlijsten zal opleveren.

Het volledig oplossen van het kennisgebrek bij afnemers is een utopie. Maar door slim gebruik te maken van bestaande tools en initiatieven, kan de kwaliteit en effectiviteit van de aanbiedersvalidatie worden verbeterd en kunnen uiteindelijk kosten in de hele keten worden bespaard, wat de consument ten goede komt met voordeligere producten. In deze whitepaper worden verschillende tools en initiatieven opgesomd die afnemende organisaties kunnen inzetten.

Ook aanbieders kunnen bijdragen aan een beter validatieproces. Meer transparantie over hun beveiligingsaanpak en een zorgvuldige invulling van hun zorgplicht kunnen het proces aanzienlijk verbeteren.

Het waarborgen van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens is essentieel om bedrijven te beschermen tegen steeds veranderende digitale dreigingen en privacyschendigen. Door samen te werken en gebruik te maken van bestaande tools kunnen we de validatieprocessen verbeteren, kosten verlagen en uiteindelijk de consument beter van dienst zijn. Transparantie en zorgplicht van aanbieders zijn cruciaal voor een effectieve en betrouwbare cyberveiligheidsketen. Samen kunnen we een veerkrachtigere toekomst bouwen en onze weg weer vinden in de complexe wereld van cyberveiligheid.

Verantwoording van de whitepaper

Deze whitepaper is tot stand gekomen door een zorgvuldige samenwerking tussen experts van het MSP-ISAC (Managed Service Provider – Information Sharing & Analysis Centre). Hierbij werd gekozen voor een expertsessie-aanpak, waarbij de focus lag op een specifieke probleemstelling: de toenemende hoeveelheid vragenlijsten die aanbieders moeten invullen.

In de voorbereidende fase hebben alle deelnemers uitgebreid informatie verzameld, die essentieel was om deze probleemstelling aan te pakken. Tijdens een intensieve workshop, waaraan alle deelnemers actief bijdroegen, werd in meerdere rondes gezocht naar de beste oplossingen en benaderingen. De sessie was bewust non-digitaal; deelnemers werkten met tastbare materialen zoals brown-papers, post-its, dot-stickers en markers. Deze aanpak diende niet alleen om ideeën te visualiseren, maar ook om de dialoog te stimuleren en dieper in te gaan op de geselecteerde thema's.