© 2024, Tesorion Nederland BV



September - 2024

De evoluerende rol van de CISO

Van technisch expert naar strategisch partner van de directie

Classificatie: publiek

Auteur: **Tesorion Nederland BV**

Auteur: **Tesorion Nederland B.V.**
Titel: De evoluerende rol van de CISO
Classificatie: publiek
Datum: Q3 2024
Versie: Versie 1

© 2024, Tesorion Nederland BV
Uitgegeven in eigen beheer
contact@tesorion.com

Vormgeving door: Graphic Lab
Fotografie door: Adobe Firefly (AI)
prompter: Graphic Lab

Alle rechten voorbehouden.
Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande, schriftelijke toestemming van de auteur.

Inhoud

1. Inleiding **5**

2. De rol van de CISO **6**

3. Naar een agenda voor de toekomst **8**

3.1 Agendapunt 1: Groei en innovatie 9
3.2 Agendapunt 2: Nieuwe Technologie 10
3.3 Agendapunt 3: Geopolitiek 11
3.4 Agendapunt 4: Risico versus werkbaarheid 12
3.5 Agendapunt 5: Energie en duurzaamheid 14

4. Conclusie **17**



AI Generated with Adobe Firefly.
Prompt: “the Eiffel Tower at night in Paris, during the Olympic Games shown from a low angle 27263.”

1. Inleiding

Ransomware, DDoS-aanvallen, grootschalige phishingcampagnes: cyberdreigingen blijven onverminderd aanwezig. Zo waren de websites van verschillende Nederlandse *provincies* dit voorjaar tijdelijk onbereikbaar door een DDoS-aanval. Bij een ransomware-aanval op een *dienstverlener* voor communicatie werden klantgegevens van een groot online warenhuis buitgemaakt. Ook het omzeilen van multifactorauthorisatie (MFA) om inloggegevens en eventuele twee factorauthenticatiecodes te onderscheppen om vervolgens te kunnen inloggen komt steeds vaker voor. En rondom de Olympische Spelen in Parijs kwamen grootschalige *phishingcampagnes* op gang, waarbij bedrijven bijvoorbeeld benaderd werden met de vraag of ze '*officieel sponsor*' van de Spelen wilden worden.



Het zijn slechts enkele voorbeelden uit de recente praktijk. Zeker nu organisaties op steeds meer manieren in contact staan met de buitenwereld en steeds vaker optrekken met partners binnen de supply chain, groeit ook het aantal 'ingangen' voor cybercriminelen. Bovendien hebben hackers dankzij artifical intelligence (AI) een heel nieuw arsenaal aan 'wapens' in handen gekregen om bedrijven en organisaties (al dan niet in de kritieke infrastructuur) aan te vallen. Het securitylandschap verandert, en daarmee ook de rol van de CISO.

Cybersecurity als randvoorwaarde voor groei

Cybercriminaliteit vormt een aantrekkelijk verdienmodel, met maatschappelijke ontwrichting en veel schade voor mensen en organisaties als gevolg. Binnen dit dynamische krachtenveld zullen bedrijven en organisaties zich staande moeten zien te houden. Tegelijkertijd staat er grote druk op organisaties om werk te maken van digitale transformatie en nieuwe technologieën – zoals AI en cloud computing – te omarmen.

Zeker in grotere organisaties is de rol van de Chief Information Security Officer (CISO) bij dit alles cruciaal. Hij of zij zorgt ervoor dat de belangrijkste systemen en data, zoals intellectueel eigendom of gegevens van medewerkers en klanten, goed beschermd zijn tegen cyberaanvallen. Van oudsher is de CISO vaak een technische, beleids- of procesmatige expert, primair gericht op informatiebeveiliging. Toch zien we deze rol steeds vaker veranderen. In de gemiddelde boardroom groeit het besef dat cybersecurity een belangrijke randvoorwaarde voor groei is, en niet alleen een noodzakelijk kwaad of wettelijke verplichting. Daarmee verandert ook het ideale profiel van de CISO steeds meer: van pure expert naar strategisch partner van de directie.

In deze visiepaper nemen we deze veranderende rol van de CISO nader onder de loep. Hoe kan de CISO bijdragen aan de strategische agenda van een organisatie? Hoe draagt deze rol bij aan het realiseren van de bedrijfsdoelstellingen? En over welke competenties dient een moderne CISO te beschikken?

bron: https://www.nu.nl/tech/6306531/cyberaanval-legt-websites-van-meerdere-provincies-plat.html
bron: https://www.dutchitchannel.nl/news/458746/bol-com-mogelijk-klantdata-gestolen-bij-aanval-addcomm
bron: https://www.techvisor.nl/Artikelen/15297/de-olympische-spelen-topsport-voor-cybercrime?list=y
bron: https://cybernews.com/news/fake-olympic-shops-fans-significant-financial-losses/

2. De rol van de CISO

Medio jaren negentig ontstond (na de opkomst van informatietechnologie en netwerken eind jaren tachtig) de rol van CISO: een medewerker die zich volledig richtte op informatiebeveiliging en de bescherming van (gevoelige) gegevens. De verantwoordelijkheden van de CISO waren met name gericht op het opstellen en onderhouden van securityprotocollen, het uitvoeren van periodieke risicoanalyses en het naleven van relevante regelgeving. Voor de rol van CISO was in die tijd goede technische kennis vereist.

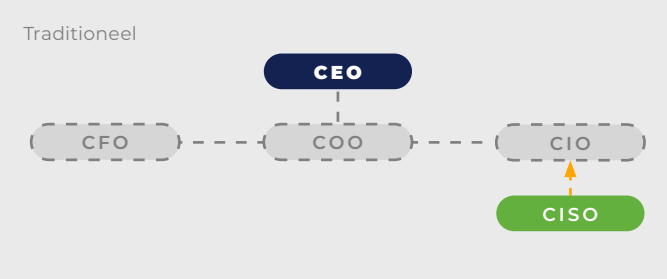
Het dreigingslandschap bleef zich in snel tempo ontwikkelen, en dat zorgde voor veranderingen in de rol van de CISO. De CISO werd ook verantwoordelijk voor beleid en risicobeheer. Om dit goed in te kunnen vullen was nauwe samenwerking nodig met leidinggevenden en directie om cybersecuritystrategieën goed af te kunnen stemmen op de bedrijfsdoelstellingen.

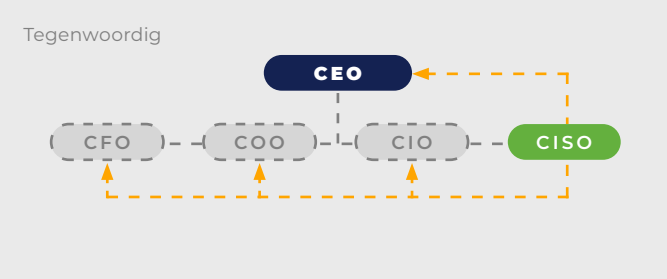
Het werkveld van de CISO was daarmee gericht op het managen van cybersecurityrisico's op het gebied van vertrouwelijkheid, integriteit en beschikbaarheid van data. Inmiddels is het IT-landschap onherkenbaar veranderd en zijn cyberdreigingen veel talrijker en complexer geworden. Ook de wet- en regelgeving op dit vlak is flink aangescherpt. Denk maar aan NIS2, de nieuwe Europese richtlijn voor cybersecurity die dit najaar ingaat en die concrete eisen op het gebied van IT-beveiliging bevat.

SAMENWERKING EN PLAATS IN DE ORGANISATIE

Traditioneel gezien rapporteert de CISO aan de Chief Information Officer (CIO). We zien echter ook dat de CISO steeds vaker samen met andere executives op C-level samenwerkt bij het formuleren van een integrale beveiligingsstrategie. Dit kan zorgen voor conflicterende belangen en voor verschillende agenda's van CIO en CISO. Zo is de CIO – vanuit zijn verantwoordelijkheid voor de algehele IT-strategie van een organisatie – vaak primair gericht op efficiëntie en kostenbesparingen, en dat kan op gespannen voet staan met structurele beveiligingseisen. Tegelijkertijd wil de CISO soms strikte beveiligingsprotocollen invoeren, maar deze kunnen IT-innovaties belemmeren door ze complexer en duurder te maken. Ook de prioriteiten van een CISO en een CEO lijken soms haaks op elkaar staan. Investeringen in cybersecurity dragen op korte termijn immers niet direct bij aan de winst; cybersecurity doe je om security-incidenten te voorkomen en zo voor zekerheid te zorgen.

Niet voor niets zien we steeds vaker dat de CISO (ook) rapporteert aan een ander bestuurs- of directielid, zoals een CFO of COO; om zijn onafhankelijkheid te waarborgen, en om ervoor te zorgen dat beveiligingskwesties voldoende gewicht krijgen in strategische beslissingen. Ook in de boardroom zal het besef moeten groeien dat cybersecurity een essentiële randvoorwaarde is voor gezonde groei op de langere termijn. Daarbij past een ruimer mandaat voor de CISO, zodat cybersecurity niet alleen op papier maar ook in de praktijk adequaat wordt ingevuld.





DE CISO BINNEN DE ORGANISATIE

Steeds meer beseft men in boardrooms dat cybersecurity geen 'IT-feestje' en een kostenpost is, maar een business enabler die in alle bedrijfsprocessen geïntegreerd moet worden. Maar: het 'uitnutten' van cybersecurity als strategisch voordeel vraagt om gespecialiseerde kennis en strategisch leiderschap. Idealiter verandert daarmee ook de rol van de CISO; van een beleidsmatig of puur technisch expert naar een strategische partner, die vanuit zijn of haar expertise kan bijdragen aan de strategische besluitvorming.



BETERE RELATIE TUSSEN CISO EN BOARDROOM

Uit recent onderzoek van *Proofpoint* blijkt dat de afstemming tussen CISO's en de raad van bestuur de laatste jaren is verbeterd. Meer CISO's en bestuursleden zijn het er nu over eens dat ze op dezelfde lijn zitten wat betreft het belang en de aanpak van cybersecurity. Zo is iets minder dan 62 procent van de CISO's het eens met de stelling dat hun raad van bestuur hetzelfde denkt over cybersecuritykwesties. Dat is een kleine stijging ten opzichte van 2021 **(59%)** en een iets grotere stijging ten opzichte van 2022 **(51%)**. Bestuursleden zelf zijn nog positiever over de relatie, waarbij **69%** het gevoel heeft dat ze op dezelfde lijn zitten.

Tegelijkertijd bestaat er nog steeds een lichte verdeeldheid rond de duiding van de gevolgen van een cyberaanval, die overeen lijkt te komen met de verschillende manieren waarop CISO's en bestuursleden kijken naar schade-elementen op de korte versus de lange termijn. CISO´s hebben de indruk dat bestuursleden zich het meest zorgen maken over reputatieschade **(36%)**, impact op bedrijfswaardering **(36%)** en verlies van huidige klanten **(36%)**. Hoewel al deze zorgen terecht zijn, komen ze niet helemaal overeen met de belangrijkste zorgen die directies zelf aangeven te hebben als gevolg van een cyberaanval. Zij noemen daarbij als belangrijkste zorgen: operationele downtime en dataherstel **(38%)**, financieel verlies **(33%)** en regelgevende sancties **(33%)**.

De zorgen van CISO's en bestuursleden staan echter wel met elkaar in verband. Zo leidt operationele downtime tot reputatieschade, en daarmee tot impact op de bedrijfswaardering en tot verlies van klanten. Alhoewel CISO's en bestuursleden dus niet altijd dezelfde zorgen bovenaan hun lijst hebben staan, komen hun zorgen vaak voort uit dezelfde onderliggende risico's. Dit benadrukt het belang van goede communicatie en samenwerking, om ervoor te zorgen dat alle aspecten van een cyberaanval worden onderkend en aangepakt.

bron: https://www.proofpoint.com/us/resources/white-papers/voice-of-the-ciso-report

AI Generated with Adobe Firefly.
Prompt: "A photo of a chief information security officer in a board room sitting in the middle of the-3."

3. Naar een agenda voor de toekomst

Idealiter loopt cybersecurity als een rode draad door alle bedrijfsprocessen heen en is iedereen op C-level doordrongen van het belang van een robuust beveiligingslandschap. De CISO speelt een cruciale rol bij het mogelijk maken van digitale bedrijfsinitiatieven, door het implementeren van een robuust en verdedigbaar cybersecurityprogramma. De voornaamste uitdaging voor de CISO daarbij is om zich te ontwikkelen van een technisch expert tot een storyteller. Hij of zij moet begrijpen welke maatregelen nodig zijn om de organisatie goed te beveiligen. Daarbij gaat het om maatregelen op zowel technisch als op organisatorisch, menselijk en procesmatig vlak.

CISO's rapporteren steeds vaker rechtstreeks aan de CEO of het bestuur. Dit heeft voordelen voor zowel de strategische doelstellingen van de organisatie als voor de cultuur van het beveiligingsteam. Met de groei van het belang van automatisering binnen het bedrijf groeit de rol van de CISO mee, waarbij qua beveiliging rekening moet worden gehouden met een steeds meer verbonden wereld. Tegelijkertijd moet de CISO óók in staat zijn om collega-bestuurders (en de rest van de organisatie) mee te nemen in het daardoor snel veranderende dreigingslandschap. Daarmee ondersteunt de CISO de strategische bedrijfsagenda, zowel vanuit een technisch perspectief (om automatisering te faciliteren) als vanuit een risicoperspectief.

Maar hoe ziet die agenda er dan precies uit? *Gartner* stelt dat de strategische agenda van de gemiddelde CEO er voor het komende jaar als volgt uitziet:

1. Groei en innovatie
2. Nieuwe technologie
3. Geopolitiek
4. Risico's versus werkbaarheid
5. Energie en duurzaamheid

In de volgende paragrafen verkennen we per agendapunt welke implicaties dit heeft voor het beleid rondom cybersecurity en de rol van de CISO. Hoe ziet die rol er idealiter uit? En waar en hoe kan de CISO echt het verschil maken?



AI Generated with Adobe Firefly.
Prompt: "A photo of a highly digital calendar. Colors- Green and Blue, Close up 76028."

bron: https://www.dutchitleaders.nl/news/437261/gartner-zes-op-de-tien-ceos-ziet-groei-als-topprioriteit

3.1 AGENDAPUNT 1: GROEI EN INNOVATIE

In hun streven naar groei, kiezen organisaties er vaak voor om te investeren in nieuwe producten, nieuwe toeleveringsketens en diversificatie om commerciële kansen te kunnen benutten. Door afscheid te nemen van ballast en zo nodig processen te vereenvoudigen, ontstaat de ruimte om te concentreren op de kernprocessen die daadwerkelijk waarde toevoegen.

De CISO speelt een belangrijke rol bij het identificeren van kernactiviteiten die essentieel zijn voor groei en efficiëntie. Innovatie is cruciaal om nieuwe kansen te ontdekken en bedrijfsmodellen te herdefiniëren. CISO's zijn betrokken bij het beveiligen van deze nieuwe technologieën, zoals AI, cloud computing en data-analyse. Zij waarborgen dat deze technologieën veilig worden geïmplementeerd en gebruikt. Ze evalueren de risico's van innovatieve projecten en helpen bij het vinden van een balans tussen innovatie en beveiliging.

De CISO zorgt ervoor dat beveiligingsinspanningen gericht zijn op wat er echt toe doet, en dat de kernprocessen worden beschermd en gefaciliteerd. Daarnaast moeten C-level executives digitale transformatie en nieuwe technologie omarmen om concurrerend te blijven en te kunnen groeien.

Nederland staat bekend als een innovatief land. Zo staat Nederland op de vierde positie in het European Innovation Scoreboard (EIS) en worden we door de EU aangemerkt als *innovatieleider*. Daarbij gaat het niet alleen om de ontwikkeling van nieuwe, innovatieve producten, maar zeker ook om procesinnovatie en digitale transformatie. Zo nemen geavanceerde robots de saaie, repeterende taken steeds vaker over. En op het snijvlak van big data, geavanceerde sensortechnologie en AI ontstaan steeds meer mogelijkheden voor datagedreven innovatie; bijvoorbeeld als het gaat om voorspellend onderhoud en voortdurende procesoptimalisatie.

Groei door innovatie

De CISO speelt een niet te onderschatten rol bij het identificeren van kernactiviteiten die essentieel zijn voor de groei van en de efficiëntie binnen de organisatie. Hij of zij bewaakt daarbij de balans tussen innovatie en beveiliging en zorgt ervoor dat nieuwe technologieën als AI veilig geïmplementeerd worden, met een minimale impact op vooruitgang en efficiëntie. Ook adviseert de CISO over eisen aan gegevensopslag in de cloud. Vanuit zijn of haar betrokkenheid bij digitale transformatie en innovatie, kun je als organisatie hierin steeds de juiste keuzes maken – voor maximaal strategische toegevoegde waarde.

Innovatie in de keten

Innovatie ontstaat steeds vaker in de keten, in nauwe samenwerking met supply chain-partners. Doordat organisaties op steeds meer manieren in contact staan met de buitenwereld en steeds vaker optrekken met partners binnen de supply chain, groeit ook het aantal 'ingangen' voor cybercriminelen. Deze toenemende ketenintegratie brengt dan ook ook risico's met zich mee. Cybercriminelen gaan in de regel op zoek naar de zwakste schakel in de keten. Als bijvoorbeeld je hostingpartij of de leverancier van je beveiligingscamera's, je printers of je toegangscontrolesysteem zijn zaakjes niet op orde heeft, kan dat zomaar betekenen dat cybercriminelen via een achterdeur alsnog kunnen binnenkomen – hoe goed je je eigen beveiligingsschil ook hebt ingericht.

Niet voor niets is er binnen de nieuwe NIS2-richtlijn aandacht voor ketenverantwoordelijkheid. Als bedrijf is het dan ook des te belangrijker dat je je (innovatie)partners en leveranciers met veel zorg selecteert. Ook hier speelt de CISO weer een niet te onderschatten rol. De CISO hoeft uiteraard niet de leveranciersbeoordeling over te nemen, maar hij of zij speelt wel een belangrijke rol bij het scheppen van de juiste kaders. Waaraan moeten partners en leveranciers minimaal voldoen? Hoe kan dit binnen het selectie- en inkoopproces geborgd worden? En hoe kan binnen de organisatie het bewustzijn rondom dit onderwerp worden vergroot? De CISO adviseert, stuurt en bewaakt.

Overnames en ketenintegratie

Groeien kan natuurlijk ook door andere organisaties over te nemen. In de regel vindt er bij overnames een due dilligence-onderzoek plaats, waarbij de koper uitgebreid in de boeken van de overnamekandidaat duikt. Naast dit onderzoek, is het daarbij ook goed om onderzoek te doen naar de beveiliging van het over te nemen bedrijf, hun securityorganisatie, processen, systemen en data. Zo voorkom je dat cyberproblemen of beveiligingsongelijkheden bij de overnamekandidaat invloed hebben op jouw eigen beveiligingslandschap. Een CISO is de aangewezen persoon om dit te onderzoeken en uiteindelijk de verschillende omgevingen bij elkaar te brengen.

bron: https://www.bedrijvenbeleidinbeeld.nl/strategische-doelen/bevorderen-van-innovatie-en-economische-vernieuwing-in-sectoren/versterken-van-innovatie-in-het-bedrijfsleven/european-innovation-scoreboard"innovatieleider

3.2 AGENDAPUNT 2: NIEUWE TECHNOLOGIE

Digitale koppelingen (zogenoemde API's). Nieuwe, datagedreven verdienmodellen. Efficiëntere bedrijfsprocessen. Een betere klantervaring. Op het snijvlak van big data en innovatieve technologieën als AI, robotisering en cloud computing ontstaan allerlei mogelijkheden voor digitale transformatie. Tal van bedrijven en organisaties zoeken naar mogelijkheden zichzelf opnieuw uit te vinden als digital enterprise en op die manier meer waarde te creëren voor hun klanten. Niet voor niets noemt Gartner nieuwe technologie – in aansluiting op het eerste agendapunt over innovatie – expliciet als belangrijk punt op de strategische agenda.

Deze vierde technologische revolutie, waarin de ontwikkelingen elkaar razendsnel opvolgen, roept vanzelfsprekend ook tal van vragen op rondom informatiebeveiliging en cybersecurity. Zo implementeren ziekenhuizen steeds vaker AI-oplossingen om de diagnostische nauwkeurigheid te verbeteren. Dit roept echter ook allerlei vragen op rondom de beveiliging van gevoelige patiëntgegevens. De inhoudelijke verantwoordelijkheid ligt bij de data- en systeemeigenaren, terwijl de aansprakelijkheid bij het bestuur ligt. Dat betekent dat je als CISO de juiste vragen moet stellen aan de direct verantwoordelijken om te kunnen voldoen aan jouw verantwoordelijkheid, namelijk het afstemmen van het beveiligingsontwerp, -implementatie en het -beheer.

Een ander voorbeeld is de implementatie van cloud computing. Deze cloudtransitie biedt schaalbaarheid en flexibiliteit, maar stelt ook nieuwe eisen aan de beveiliging van gegevens en de naleving van privacywetgeving. Een derde voorbeeld is de opkomst van (IoT)-technologieën in industriële omgevingen. Fabrikanten implementeren slimme sensoren om hun productielijnen te optimaliseren en voorspellend onderhoud mogelijk te maken. De CISO moet in deze context toezien op de beveiliging van de netwerken die deze apparaten verbinden, om voldoende weerstand te bieden tegen cyberdreigingen zoals ransomware-aanvallen.

Cruciale rol

Kijkend naar de mate waarin innovatie impact heeft op de bedrijfsdoelstellingen blijkt dat er een cruciale strategische rol is weggelegd voor de CISO, waarbij deze uiteraard voldoende mandaat moet krijgen. In zijn nieuwe strategische rol moet de CISO zowel de taal van de techniek als die van de business kunnen spreken. Hij denkt niet alleen in risico's, maar ook in kansen. Zo kan de CISO een essentiële rol spelen bij het selecteren van nieuwe software en technologieën. Ook borgt hij dat deze veilig kunnen worden geïmplementeerd en gebruikt, in lijn met de beveiligingseisen van de organisatie. De CISO evalueert de risico's van innovatieve projecten en helpt zo bij het vinden van een balans tussen innovatie en beveiliging.

Voor CEO's is het op hun beurt belangrijk om hun CISO vanaf het begin mee te nemen in de ideeën die er zijn voor de inzet van bijvoorbeeld AI, cloud computing of slimme meet- en regelapparatuur.

DE OPKOMST VAN DE CHIEF AI OFFICER (CAIO)

De rollen van CIO en CISO verschuiven van puur technische functies naar strategische posities. CISO's moeten nu AI-technologieën integreren, en strategische cybersecurity en bedrijfsontwikkeling combineren. CISO's moeten daartoe nieuwe vaardigheden ontwikkelen, om AI te kunnen begrijpen en te implementeren. Dit omvat het evalueren van AI-systemen en het aanpassen daarvan aan de behoeften van hun organisatie.

Er ontstaat daarbij een nieuwe rol, de Chief AI Officer (CAIO), die verantwoordelijk is voor AI-initiatieven en het optimaliseren van datagebruik. In veel organisaties nemen CIO's voorlopig deze rol op zich. Zij moeten daarin samenwerken met CISO's om een balans te vinden tussen digitale transformatie en dataveiligheid. Dit vereist een cultuur van *security first*, die aansluit bij de bedrijfsdoelen.

CISO's moeten zich voorbereiden op een toekomst waarin AI een cruciale rol speelt in bedrijfsstrategieën. Dit betekent dat ze moeten bijscholen en zich moeten aanpassen aan veranderende technologieën en bedrijfsmodellen. Deze veranderingen benadrukken het belang van strategisch denken en samenwerking tussen CIO's en CISO's in het AI-tijdperk.

3.3 AGENDAPUNT 3: GEOPOLITIEK

De oorlog tussen Oekraïne en Rusland, het in alle hevigheid opgelaaide Palestijns-Israëlische conflict en de oplopende spanningen tussen China en Taiwan, maar ook eenmalige gebeurtenissen als de Olympische Spelen in Parijs en de Amerikaanse presidentsverkiezingen van 2024: ze zorgen momenteel voor een uniek dreigingslandschap, waarbij zowel fysiek als online strijd wordt gevoerd. Daarbij valt vooral het grote aantal DDoS-aanvallen op, waarbij servers worden bestookt met zulke grote hoeveelheden informatie dat ze crashen.

Kritieke infrastructuur en cyberspionage

Statelijke actoren en hacktivisten richten hun pijlen vooral op kritieke infrastructuur, zoals drinkwaterbedrijven, zorginstellingen en energieleveranciers. Hun doel: spioneren, klaar zijn voor potentiële ontwrichting van de maatschappij. Maar ook organisaties die lastige geopolitieke relaties hebben, in (potentiële) conflictgebieden zitten of zich politiek uitspreken, worden steeds vaker het slachtoffer van cybercrime – met alle gevolgen van dien voor hun bedrijfscontinuïteit en die van hun ketenpartners.

Ook het stelen van hoogwaardige kennis en intellectueel eigendom is een belangrijk doel van buitenlandse hackers. Kennis over nieuwe technologieën, producten of processen is enorm waardevol; voor landen, maar ook voor 'gewone' hackers die de buitgemaakte kennis vaak voor veel geld kunnen doorverkopen. Daarnaast zijn er ook nog cybercriminelen die opportunistisch te werk gaan en die zich richten op het buitmaken van data die geld opleveren op het dark web, zoals wachtwoorden en persoonsgegevens. Deze data kunnen vervolgens weer door statelijke actoren gebruikt worden bij het realiseren van hun doel.

Phishing-campagnes: steeds geraffineerder

Events als de Olympische Spelen en de Amerikaanse verkiezingen leiden ook tot een toename van het aantal phishing-campagnes, waarbij bedrijven en organisaties op geraffineerde wijze worden opgelicht. Een voorbeeld: tal van bedrijven kregen in de aanloop naar de Spelen in Parijs de vraag of ze 'officieel sponsor' van het evenement wilden worden. Dankzij *AI-tools*[1] als ChatGPT kunnen cybercriminelen daarbij steeds geraffineerder te werk gaan, en de verwachting is dat aanvallen in de toekomst alleen maar realistischer zullen worden door de groeiende mogelijkheden voor bijvoorbeeld deepfakes en het zeer realistisch nabootsen van stemmen. Voor organisaties zal het steeds lastiger worden om onderscheid te maken tussen 'echt' en 'nep'.

Nepnieuws

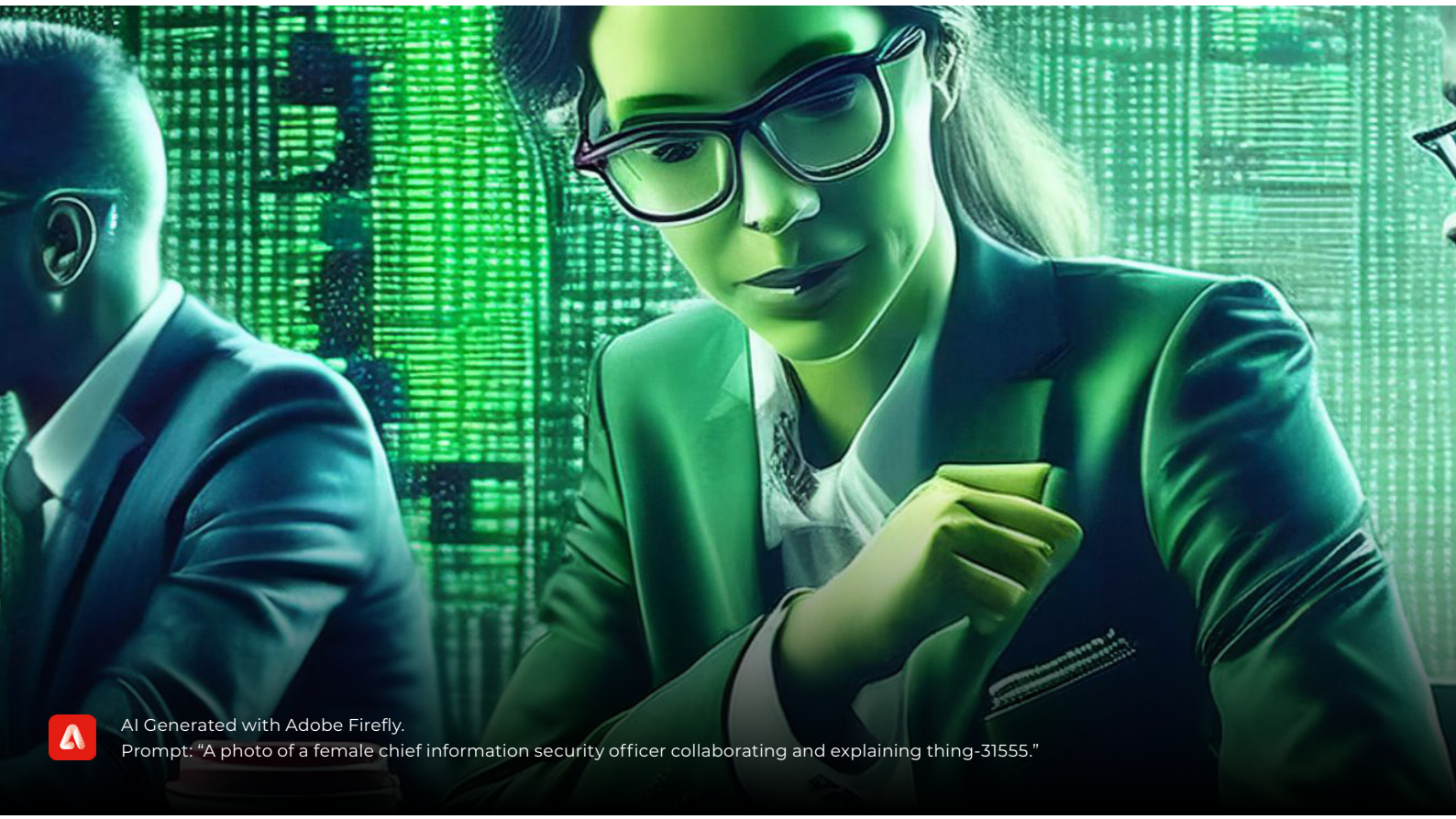
Ten slotte neemt rondom grote evenementen vaak ook de hoeveelheid desinformatiecampagnes toe. Zo ontstond in het najaar van 2023 'massahysterie' rondom een vermeende bedwantsenplaag in Parijs. Uiteindelijk bleken het met name Russische trollen te zijn geweest die dit alarmerende nepnieuws de wereld in hadden geholpen. Ook rondom belangrijke verkiezingen neemt de hoeveelheid nepnieuws vaak significant toe, in een poging om verkiezingsuitslagen te beïnvloeden en het brede sentiment in de samenleving te sturen (moderne propaganda).

CISO als verbindende schakel

Waar bedrijven en organisaties die zich bezighouden met kritieke infrastructuur zich doorgaans goed bewust zijn van de (door geopolitiek ingegeven) dreigingen en ook de bijbehorende securitymaatregelen in acht nemen, ligt dat anders bij het gemiddelde Nederlandse MKB-bedrijf. Vaak ontbreekt op C-level een collega die de verbindende schakel vormt tussen de operatie van alledag en het toenemende aantal dreigingen van buiten. Tegelijkertijd zit dit soort organisaties vaak diep genesteld in een toeleveringsketen aan de kritieke infrastructuur.

De rol van verbindende schakel is er een die de CISO goed op kan pakken. Uiteraard door er in technische zin voor te zorgen dat het aanvalsoppervlak kleiner wordt, maar ook in strategisch opzicht speelt de CISO een onmisbare rol. In de eerste plaats door voortdurend zelf de dreigingsomgeving te monitoren, inclusief de opkomst van nieuwe (geopolitieke) dreigingen en mogelijk kwaadaardige activiteiten. Maar ook door het opbouwen en onderhouden van relaties met externe partners, zoals cybersecurity-experts, overheidsinstanties en andere organisaties in de sector. Dit netwerk kan van onschatbare waarde zijn bij het delen van informatie over dreigingen en bij de communicatie rond de aanpak van grootschalige incidenten.

[1] *bron: Zie onze eerdere paper De kracht van AI in cybersecurity (Tesorion, 2024): https://www.tesorion.nl/nl/thema/artificial-intelligence-in-cybersecurity/*



AI Generated with Adobe Firefly.
Prompt: “A photo of a female chief information security officer collaborating and explaining thing-31555.”

3.4 AGENDAPUNT 4: RISICO VERSUS WERKBAARHEID

Proactief risico’s identificeren en beheren is essentieel. Veerkrachtige bedrijfsmodellen zijn cruciaal voor organisaties om zich aan te passen aan veranderende geopolitieke omstandigheden. De CISO heeft daarbij de rol om robuuste cybersecurityprogramma’s te ontwikkelen en te implementeren om gegevens en systemen te beschermen. Solide incidentresponsplannen zijn natuurlijk een belangrijk thema om de organisatie veerkrachtig te maken. Maar de CISO is vanuit zijn ervaring met het beoordelen en prioriteren van risico’s ook een gids voor de bestuurskamer in het navigeren van de organisatie door een dreigingslandschap, bijvoorbeeld onder invloed van geopolitieke ontwikkelingen. Het kunnen communiceren van risico’s is daarbij essentieel.

Een calamiteit is een mogelijke impact waar geen effectief, compleet maatregelpakket tegen te nemen is. In een calamiteitenplan wordt vastgelegd hoe met dat soort situaties om te gaan. In de gemiddelde boardroom wordt de impact van cyberincidenten in de praktijk echter vaak nog onderschat. Zeker organisaties die nog nooit zelf te maken kregen met een aanval, hebben vaak geen calamiteitenplannen klaarliggen. Wat doe je bijvoorbeeld wanneer er klantgegevens op straat komen te liggen, er een productielijn stilvalt door malware of intellectueel eigendom wordt gestolen? Terwijl die incidenten wel een enorme impact kunnen hebben, zowel op financieel niveau als qua reputatieschade. En is er wel een calamiteitenplan, dan wordt dit vaak niet geactualiseerd en/of regelmatig geoefend.

Balans bewaken

De traditionele rol van de CISO is om ervoor te zorgen dat aan alle basale securitymaatregelen – zoals multi-factorauthenticatie, netwerksegmentatie, versleuteling en regelmatige updates – is voldaan. Tegen de achtergrond van een steeds sneller veranderend dreigingslandschap en een steeds grotere afhankelijkheid van IT, is het aan de CISO om, binnen deze voortdurend veranderende context, de balans te bewaken. Een CISO is van oudsher bezig met risico’s en maatregelen. Deze situatie verandert naar een situatie waarbij het uitgangspunt voor de CISO een business impactanalyse (BIA) is, om vervolgens een risicoanalyse of calamiteitenplan te kunnen schrijven waar tegenwoordig ook de



Risico:
Kans dat een incident plaatsvindt * Impact op organisatie

bedrijfscontinuïteit onderdeel van is. Dat betekent het vastleggen van de mogelijke impact van een risico op het bedrijfsbelang van een organisatie.

Ook houdt hij of zij de belangrijkste ontwikkelingen op het gebied van cybersecurity bij en doorgrondt de CISO de bijbehorende risico's, om dit vervolgens vast te leggen in een goed onderbouwd, regelmatig te actualiseren risicobehandelplan. Daarbij bewaakt de CISO goed de balans tussen de geïdentificeerde risico's en de bijbehorende impact, de praktische uitvoerbaarheid van bepaalde maatregelen én – uiteraard – de kosten. Zo kunnen CISO's ervoor kiezen om, bij systemen met lage impact, softwareupdates meteen automatisch te installeren. Voor systemen die kritiek zijn voor de bedrijfsvoering is het verstandig om de update eerst te testen in een geïsoleerde omgeving of in stappen uit te rollen, om te bepalen of er geen ongewenste bijwerkingen zijn; denk maar aan de wereldwijde storing in Windows-computers, afgelopen juli, na een foutieve update door cybersecuritybedrijf *CrowdStrike*. Door een update van kritieke systemen gefaseerd en gecontroleerd uit te voeren, verkleinen CISO's het risico op een onderbreking van de kritieke bedrijfsprocessen.

De CISO als storyteller

Maar: daarmee is de CISO er nog niet. Hij of zij moet ook goed kunnen communiceren en als storyteller de directie meenemen in de relevante scenario's. Wat betekent een incident voor de bedrijfsvoering? En wat is er nodig om de impact zoveel mogelijk te beperken? De moderne CISO heeft kennis van verandermanagement; hij of zij weet hoe de psyche van de mens werkt en kan goed inschatten hoe mensen zullen reageren op bijvoorbeeld een cultuurwijziging of gewenste gedragswijzigingen. Zo zet de CISO cybersecurity met zijn didactische skills op de agenda én weet deze daar te houden.

Wat daarbij wellicht helpt, is dat directieleden onder de nieuwe NIS2-wetgeving verplicht zijn om zich nader te informeren op het gebied van informatiebeveiliging. Die toenemende awareness leidt naar verwachting tot een beter, constructiever gesprek tussen de boardroom en de CISO.

bron: https://nos.nl/artikel/2529477-wat-is-crowdstrike-en-hoe-kon-het-zo-misgaan-dit-is-wat-we-nu-weten

3.5 AGENDAPUNT 5 : ENERGIE EN DUURZAAMHEID

CEO's moeten een duidelijke missie, visie en strategie communiceren. Dit trekt talent aan, bevordert de betrokkenheid van medewerkers, en zorgt voor vertrouwen bij klanten en investeerders. De CISO draagt bij aan die talentontwikkeling door te investeren in het opleiden en ontwikkelen van beveiligingsprofessionals. Daarnaast communiceert de CISO duidelijk hoe het security-office aan de bedrijfsmissie en strategie bijdraagt. Door uit te leggen hoe het security-office aansluit op en bijdraagt aan deze gezamenlijke strategie, groeien de betrokkenheid en het vertrouwen op het gebied van cybersecurity. Ook het ontwikkelen van de bewustwording rond thema's als cyberdreigingen is belangrijk.

Organisaties moeten ook duurzaamheid integreren in hun bedrijfsstrategie. Dit omvat milieuvriendelijke praktijken, sociale verantwoordelijkheid en goed bestuur. De CISO speelt bijvoorbeeld een belangrijke rol tijdens het selectieproces van nieuwe leveranciers en het duurzaam kunnen benutten van nieuwe energiebronnen. Daarnaast kun je als CISO bij maatregelkeuzes rekening houden met bijvoorbeeld klimaatneutraliteit en circulariteit. Leveranciers kunnen daarbij ook beoordeeld worden op hun duurzaamheid, inclusief de supply chains. Bijkomend voordeel: omdat je als CISO breed in het bedrijf contacten hebt, kun je zeker helpen dit breed uit te dragen binnen het bedrijf.

Klimaatverandering en duurzaamheid staan wereldwijd hoog op de maatschappelijke en politieke agenda. Ook in Nederland zoeken organisaties – daartoe aangespoord door wet- en regelgeving en door klanten, leveranciers en partners – naar manieren om hun ecologische voetafdruk te verkleinen, het circulair gebruik van grondstoffen te bevorderen en arbeidsomstandigheden te verbeteren; denk bijvoorbeeld aan initiatieven voor talentontwikkeling (een leven lang leren).

OT-apparatuur

Om hun bedrijfsprocessen duurzamer en efficiënter te maken, investeren steeds meer organisaties in slimme automatisering. Ook zetten ze bijvoorbeeld slimme meters in voor het regelen van temperatuur en licht in een gebouw, laadpalen voor een elektrisch wagenpark, of zonnepanelen en omvormers voor het opwekken van hernieuwbare energie. Dat betekent dat er meer OT-apparatuur wordt aangesloten, en deze apparatuur kan een beveiligingsrisico vormen voor de rest van de organisatie als zij zomaar aan het bedrijfsnetwerk wordt gekoppeld. Onderhoud vormt daarbij een aanvullend cyberrisico; als je het onderhoud laat uitvoeren door externe partijen, is het belangrijk om de toegang voor leveranciers goed te regelen. Vanuit zijn of haar technische en organisatorische expertise is de CISO idealiter in staat om te bepalen in hoeverre nieuwe systemen de bedrijfsvoering al dan niet onnodig blootstellen aan mogelijke risico's. Oftewel: de kansen die de nieuwe systemen bieden moeten opwegen tegen de veranderingen in het risicolandschap door die systemen, en het resultaat moet binnen de risk appetite van de organisatie blijven.

Lerende organisatie

Duurzaamheid is een ruim begrip waarbij de duurzame inzet van medewerkers en het continue ontwikkelen van kennis niet mag ontbreken. Onderdeel daarvan is het kweken van awareness en het opleiden en trainen van medewerkers om hen cyberweerbaar te maken. Daarbij kun je als CISO ook duurzaamheidsthema's of groene technieken introduceren en deze onderdeel maken van het aangeboden programma. Maak medewerkers bewust van de manieren waarop cybercriminelen inspelen op actuele thema's en deze gebruiken om te *phishen*, en benadruk het omgaan met gevoelige informatie en dataclassificatie in leverancierssketens.



AI Generated with Adobe Firefly.
Prompt: "A photo of a smart device, which increases efficiency in a factory. colors: green and blue."



ONDERZOEK: CYBERSECURITY IN DE ZONNESECTOR

In Nederland wordt steeds meer gebruikgemaakt van duurzame energiebronnen, zoals zonne-energie. Omdat zonne-energie een steeds groter deel uitmaakt van de totale energievoorziening in Nederland, heeft RVO (Rijksdienst voor Ondernemend Nederland) de samenwerking gezocht met de Topsector Energie (energie-experts) en Secura (cybersecurity-experts) voor een onderzoek naar cybersecurity in de zonnesector.

In augustus 2024 is het *onderzoeksrapport* gepubliceerd. Citaat uit dit rapport: “Het onderzoek heeft geleid tot 27 scenario’s die kunnen leiden tot grootschalige verstoring van de zonnestroomsector. Daarnaast is geconstateerd dat dergelijke verstoringen ook effect zullen hebben op de gehele energiesector en dat sommige scenario’s ook effecten zullen hebben buiten de zonnestroomsector. Hoewel over de kans van een succesvolle aanval gediscussieerd kan worden, is de potentiële impact van deze scenario’s desastreus te noemen. Er is veelal sprake van grote economische schade, fysieke schade en zelfs maatschappelijke schade. Zeker wanneer de secundaire gevolgen van de cyberaanval ook meegenomen worden.”

bron: https://topsectorenergie.nl/nl/kennisbank/maatregelen-cyberveiligheid-zonpv/

AI Generated with Adobe Firefly.
Prompt: “ A photo of renewable energy sources like solar panels and windmills. Colors green and blue 3”



AI Generated with Adobe Firefly.
Prompt: “A photo of a group of hackers as robbers standing around a table. colors: green and blue.”

4. Conclusie

Organisaties worden steeds vaker geconfronteerd met cyberaanvallen die direct of via toeleveranciers plaatsvinden. Vaak heeft zo'n cyberincident een enorme impact. Denk maar aan de ernstige cyberaanval op de *Universiteit Maastricht (UM)*, waarbij criminelen toegang kregen tot kritieke systemen en deze versleutelden. De universiteit was gedwongen losgeld te betalen en liep ernstige reputatieschade op. Ook de *KNVB* betaalde vorig jaar een flink bedrag aan losgeld, nadat een hackersgroep grote hoeveelheden vertrouwelijke persoonsgegevens wist buit te maken. En na een hack bij satellietbedrijf *Eutelsat* was er dit voorjaar kortstondig Russische propaganda te zien op de Nederlandse kinderzender BabyTV.

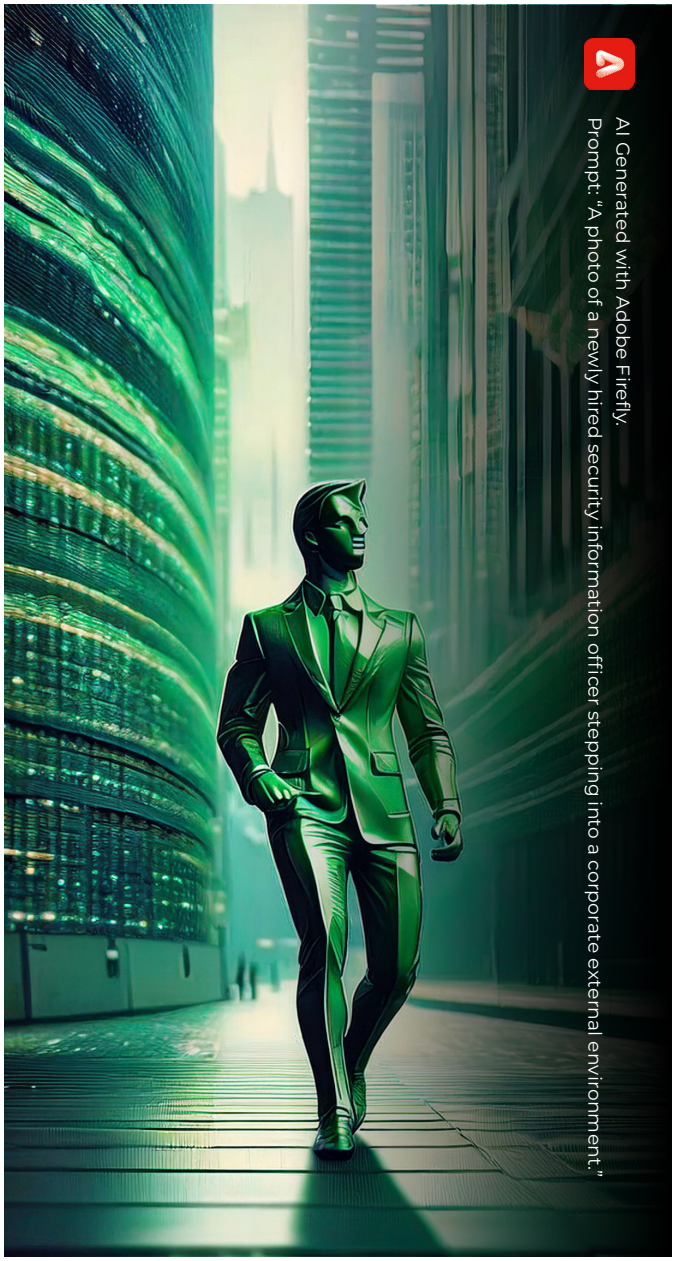
Het zijn slechts enkele voorbeelden die laten zien hoe ernstig en wijdverspreid de gevolgen van cyberaanvallen kunnen zijn, en dat geen enkele organisatie immuun is voor de impact. Met de komst van de nieuwe Europese NIS2-richtlijn dit najaar, met flink aangescherpte eisen op het gebied van IT-beveiliging, is de urgentie om cybersecurity op de agenda van de directievergadering te zetten bovendien alleen maar groter geworden.

Binnen dit krachtenveld heeft de rol van de CISO alleen maar aan gewicht gewonnen. Van een puur technische functie verandert de rol van de CISO in een strategische positie, die cruciaal is voor het succes en de veiligheid van de hele organisatie. De evolutie van de CISO-rol weerspiegelt de veranderende aard van cyberdreigingen en de groeiende erkenning van cybersecurity als cruciale randvoorwaarde voor gezonde groei.

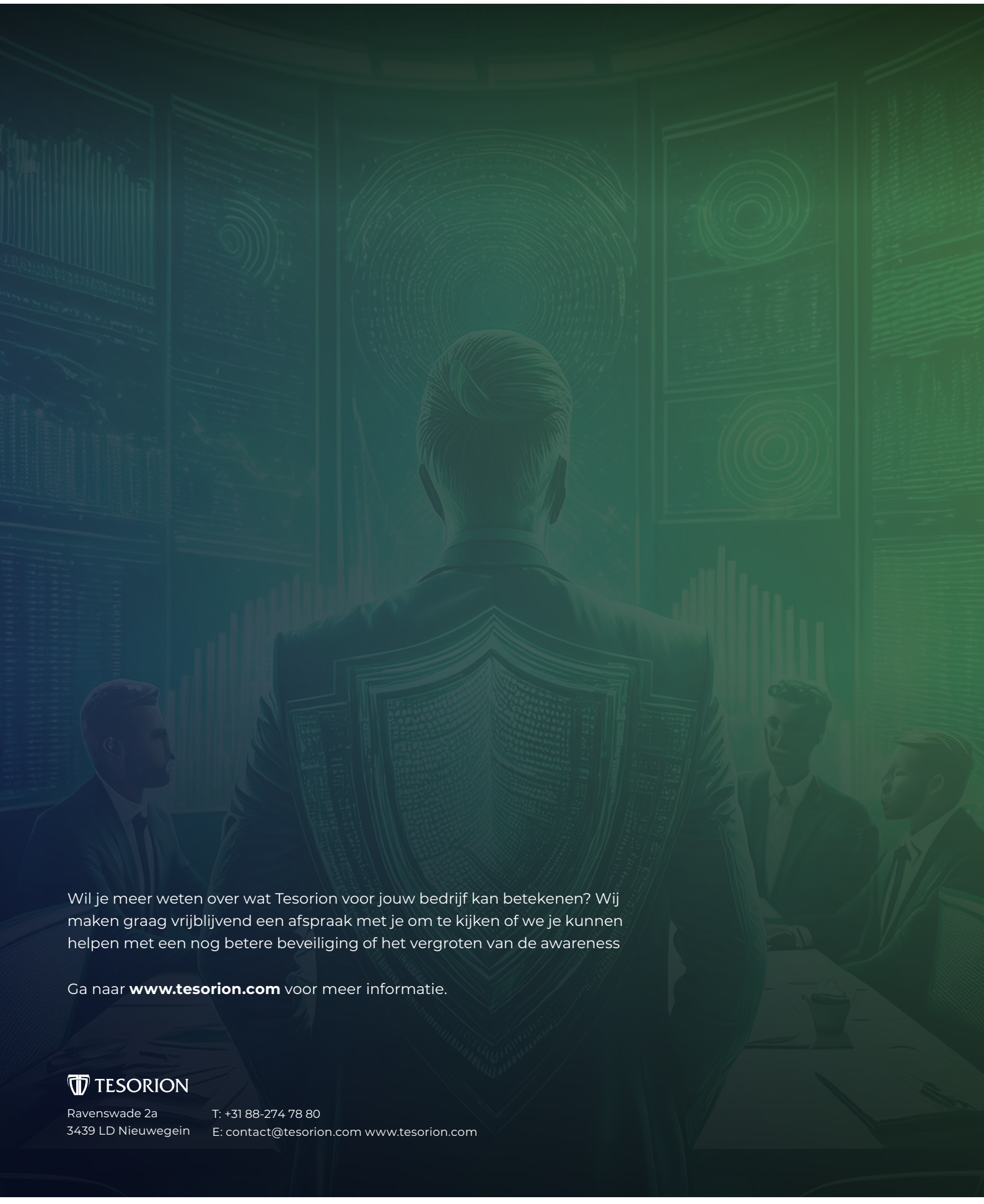
Althans: zo zou het móeten zijn. Maar nog lang niet elke organisatie heeft een CISO. En bij organisaties die dat wel hebben, blijft zijn of haar rol toch nog vaak steken in de traditionele, technische of procesmatige benadering. In deze paper hebben we hopelijk duidelijk weten te maken hoe belangrijk het is dat de CISO nauw betrokken is bij de strategische besluitvorming en dat hij of zij een volwaardige stem krijgt aan de bestuurstafel. Ook hebben we duidelijk proberen te maken waar en hoe de CISO een onmisbare rol zou kunnen spelen bij het op een veilige manier realiseren van bedrijfsdoelstellingen.

Hiervoor moet de moderne CISO over behoorlijk wat kwaliteiten beschikken. Naast diepgaande technische kennis zal hij of zij moeten beschikken over overtuigingskracht, kennis van verandermanagement en didactische skills. Ook moet hij of zij beschikken over de natuurlijke drive en nieuwsgierigheid om alle trends en ontwikkelingen binnen cybersecurity bij te houden en deze op de juiste manier te vertalen naar de boardroom en – van daaruit – de werkvloer.

Zeker op de huidige arbeidsmarkt kan het lastig zijn om iemand te vinden die aan dit profiel voldoet. Maar in een tijd waarin cybersecurity niet langer een noodzakelijk kwaad of een wettelijke verplichting is, maar een essentiële voorwaarde voor groei, is investeren in de CISO-rol een no-brainer.



bron: https://www.maastrichtuniversity.nl/nl/cyberaanval-een-samenvatting
bron: https://nos.nl/artikel/2490181-knvb-betaalt-losgeld-aan-hackers-om-vertrouwelijke-gegevens-te-beschermen
bron: https://nos.nl/artikel/2515707-russische-propaganda-te-zien-op-kinderzender-in-nederland-na-verstoring-door-hackers



Wil je meer weten over wat Tesorion voor jouw bedrijf kan betekenen? Wij maken graag vrijblijvend een afspraak met je om te kijken of we je kunnen helpen met een nog betere beveiliging of het vergroten van de awareness

Ga naar **www.tesorion.com** voor meer informatie.

TESORION

Ravenswade 2a
3439 LD Nieuwegein

T: +31 88-274 78 80
E: contact@tesorion.com www.tesorion.com