CHIEF INFORMATION SECURITY OFFICER (CISO)

Functieprofiel

DECEMBER 2025

INTEREXCELLENT
Amalialaan 41, 3743 KE Baarn

CHIEF INFORMATION SECURITY OFFICER (CISO)

Voor onze opdrachtgever CZ Groep (CZ) zijn we op zoek naar een stevige, inspirerende en verbindende *Chief Information Security Officer (CISO).* Door de snel veranderende digitale omgeving, de toenemende dreigingen en druk vanuit externe wet- en regelgeving worden steeds hogere eisen gesteld aan de informatiebeveiliging. Dit vraagt om een stevige en onafhankelijke positionering van de CISO die strategisch leiderschap toont op het gebied van digitale operationele weerbaarheid.

Als CISO ben je verantwoordelijk voor het ontwikkelen van visie, beleid en kaders, evenals het proactief identificeren, analyseren en mitigeren van security risico's. De CISO waarborgt de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van bedrijfskritische informatie en systemen.

OVER CZ

CZ is in 1930 opgericht om iedereen goede zorg te bieden tegen een betaalbare premie. Nu, ruim 90 jaar later, is dat nog steeds hun drijfveer. Waar ze ooit begonnen met 7.500 leden, zijn ze na een reeks samenwerkingen en fusies, uitgegroeid tot een zorgverzekeraar met ongeveer 2500 medewerkers die dagelijks klaar staan voor haar 4 miljoen verzekerden. CZ is een Onderlinge Waarborgmaatschappij. Dit houdt in dat CZ volledig in het belang van haar leden (de verzekerden) werkt en geen winstdoelstelling heeft.

Werken bij CZ is werk met betekenis: CZ doet alles voor zorg die verder gaat. Voor haar klanten, de zorgsector en voor de maatschappij als geheel. CZ wil verzekerden helpen om binnen de maximaal aanvaardbare wachttijd toegang tot de voor hen juiste zorg te krijgen, tegen een betaalbare premie. Dit vraagt om collega's die met plezier bijdragen en die samen met de toekomstige CZ-collega's de zorg willen innoveren. Betrokken en daadkrachtig wordt gewerkt aan kansen voor vernieuwing en verbetering van de zorg. Zo blijft de zorg betaalbaar, toegankelijk en van hoge kwaliteit gehouden. Met diezelfde mentaliteit worden verzekerden geholpen naar de beste begeleiding en de best passende zorg.

CZ STRATEGIE 2030 & DIGITALISERING

De zorgsector staat voor grote maatschappelijke uitdagingen. Door o.a. vergrijzing is er sprake van een toenemende zorgvraag maar ook een toenemend tekort aan zorgpersoneel. Daardoor staat de houdbaarheid en toegankelijkheid van gezondheidszorg onder druk en daarmee de kosten en kwaliteit van zorg. Om haar kerntaak en maatschappelijke opdracht blijvend te realiseren heeft CZ de strategie voor 2030 opgesteld, die uitgaat van een versnelling die nodig is om de komende jaren toe te groeien naar een robuuste en gelijktijdig wendbare organisatie.
Hier horen ook vernieuwingen in het IT-landschap bij. Standaardisatie, schaalbaarheid, modulariteit en veiligheid (informatiebeveiliging en cyber weerbaarheid) zijn hierin cruciale pijlers. Daarnaast richt CZ dit vernieuwde landschap zo in dat ze ook de kracht van data optimaal kunnen benutten.

CZ blijft investeren in digitalisering om diverse redenen. Enerzijds het toegankelijk houden van de eigen dienstverlening, omdat ook CZ Groep last heeft van de arbeidsmarktkrapte en ze hun diensten zodanig moeten inrichten dat ze ook met minder mensen dezelfde service kunnen blijven leveren aan hun verzekerden. Anderzijds komen ze met digitalisering, inclusief de impact van AI, tegemoet aan klantverwachtingen rondom snelheid en gemak van dienstverlening. De focus komt daarmee te liggen op digitalisering waarmee CZ het verschil kan maken.

DIVISIE DATA & IT
CZ heeft een ambitieuze strategie om de zorg toegankelijk en betaalbaar te houden. Voor het realiseren van de 2030 strategie is Data & IT een belangrijke enabler. Door het neerzetten van een schaalbaar, modulair en veilig landschap werkt CZ aan een IT omgeving die toekomstbestendig is en een belangrijke bijdrage levert aan het realiseren van de strategie.

Om dit te bereiken, zet CZ verschillende veranderingen in gang, waaronder de grootschalige vervanging van het Data & IT-landschap naar standaard platformen en de introductie van een nieuwe werkwijze ('way-of-working'). Alleen door op een nieuwe, vereenvoudigde en divisie-overstijgende manier samen te werken, kan de technologie toekomstbestendig worden geïmplementeerd.
De noodzakelijke versnelling vanuit deze strategie is niet te realiseren binnen de huidige 'way-of-working' en vraagt om een ***transformatie*** vanuit stevig leiderschap. CZ heeft daarom voor een operating model gekozen dat uitgaat van zoveel mogelijk standaardisatie en differentiatie waar het bijdraagt aan de strategie. De divisie Data & IT gaat maximaal inzetten op marktstandaarden in plaats van alles zelf te doen en transformeert daarmee naar een regie-organisatie.

Data & IT richt zich op de besturing van standaard technologieplatformen en de integratie daartussen. De organisatie voert zelf geen bouw- en ontwikkelactiviteiten uit ten aanzien van applicaties of IT infrastructuur, tenzij noodzakelijk om strategisch onderscheidende CZ activiteiten te ondersteunen.

De divisie Data & IT bestaat uit zo'n 400 FTE en is ingedeeld in een aantal organisatieonderdelen:
1. CIO Office (met o.a. een team Informatiebeveiliging);
2. Data;
3. Business domeinen: Operations, Zorg, Klant & Markt;
4. Tech Enablement (met o.a. een SOC).

Data & IT werkt in multidisciplinaire teams, waarin Business, Data en IT kennis samen komen. Deze teams dragen verantwoordelijkheid voor een product of dienst, werken zoveel mogelijk autonoom. De multidisciplinaire teams gaan werken binnen waardestromen. Een waardestroom heeft een eindverantwoordelijkheid en mandaat voor het leveren van de waarde aan klanten en realiseert een deel van de CZ strategie.

INFORMATIEBEVEILIGING EN POSITIONERING CISO
Deze nieuwe 'way of working' houdt in dat de verantwoordelijkheid voor Data & IT naar de business wordt verplaatst. Dit vereist duidelijke richting, kaders en handhaving en regie vanuit Data & IT, ook op het gebied van informatiebeveiliging.

Door de snel veranderende digitale omgeving en de toenemende dreigingen op het gebied van informatiebeveiliging worden steeds hogere eisen gesteld aan CZ. Nieuwe (Europese) wet- en regelgeving, waaronder de Digital Operational Resilience Act (DORA), verplicht CZ tot een aantoonbare en proactieve inzet op het gebied van digitale weerbaarheid en informatiebeveiliging. Ook toezichthouders scherpen hun verwachtingen aan met betrekking tot de governance, aansturing en controle op informatiebeveiliging binnen organisaties. Om meer sturing te geven aan informatiebeveiligingsstrategie en -beleid is ervoor gekozen om de CISO strategisch te positioneren en rechtstreeks aan de CIO (tevens bestuurder Data & IT) te laten rapporteren. De CISO wordt

hiermee een directe adviseur van het Bestuursteam. Het mandaat en de verantwoordelijkheden van de CISO zijn vastgelegd in het informatiebeveiligingsbeleid. Gezien de complexiteit van de dreigingen en toenemende externe druk vanuit wet- en regelgeving is deze onafhankelijke positie cruciaal.

FUNCTIE
De Chief Information Security Officer (CISO) is verantwoordelijk voor het strategisch leiderschap op het gebied van digitale operationele weerbaarheid. Dit omvat het ontwikkelen van visie, beleid en kaders, evenals het proactief identificeren, analyseren en mitigeren van security risico's. De CISO waarborgt de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van bedrijfskritische informatie en systemen.

De CISO draagt zorg voor de vertaling van security risico's naar strategische impact voor het bestuur, en fungeert als onafhankelijk adviseur van het bestuur en de Raad van Commissarissen op het gebied van (informatie)beveiliging en digitale weerbaarheid. Cruciaal hierbij is het ontwikkelen en onderhouden van een alomvattend Digital Operational Resilience Strategy (DORS) en ICT-risicobeheersingskader dat aantoonbaar voldoet aan de wettelijke eisen van de Digital Operational Resilience Act (DORA), overige wet- en regelgeving en richtlijnen van de diverse toezichthouders, waaronder van De Nederlandsche Bank (DNB).

Daarnaast is de CISO verantwoordelijk voor:

- Het stimuleren en verankeren van een organisatiebrede cultuur van beveiligingsbewustzijn en verantwoord gedrag op alle niveaus.
- Functionele sturing aan alle security gerelateerde functies (zoals team Informatie Beveiliging, SOC, IAA, etc). Betrokken bij de teamopbouw (werving en selectie) van het team Informatiebeveiliging.
- Het strategisch beheren van risico's die voortvloeien uit de afhankelijkheid van externe ICT-dienstverleners, inclusief het waarborgen van compliance met relevante wet- en regelgeving, o,a, DORA, inclusief in de toeleveringsketen. Is daarmee ook formeel eigenaar van het NOREA DORA In Control Framework.
- Eindverantwoordelijk voor het informeren en adviseren van het CZ-bestuursteam in het kader van het CZ security profiel middels de periodieke CZ Security rapportage en het CZ Dreigingsbeeld.
- Eindverantwoordelijk voor de adequate werking van het incidentresponsproces en het waarborgen van de businesscontinuïteit tijdens en na een security incident, met een focus op snelle recovery en minimale impact. Heeft een actieve leidende rol bij security incidenten met een hoge significantie, waarbij o.a. meldingsplicht geldt naar de diverse toezichthouders.
- Het implementeren van periodieke, geavanceerde weerbaarheidstesten, waaronder Threat-Led Penetration Testing (TLPT) conform het TIBER-EU framework, om de effectiviteit van de verdedigingsmechanismen continu te valideren. Is daarmee ook eindverantwoordelijk voor een actuele en geaccordeerde CZ-Digital Operational Resilience Testing (DORT) strategie/programma.
- Verantwoordelijk voor de Permanente Educatie van het CZ-bestuursteam, en Raad van Commissarissen, in het kader van Security en Digitale Operationele weerbaarheid.
- Verantwoordelijk voor budgettering i.h.k.v. Security programma's en/of projecten (niet voor lijnbudget).

De CISO opereert met een helder mandaat en voldoende autoriteit om de organisatie te leiden in het steeds volatieler wordende dreigingslandschap en draagt bij aan de toekomstbestendigheid en reputatie van CZ.
Als senior adviseur van het bestuur speelt de CISO een cruciale strategische rol. De CISO adviseert het bestuur op basis van analyses en inzichten omtrent informatiebeveiliging, risicobeoordelingen en de algehele digitale operationele weerbaarheid van de organisatie. Dit advies helpt bij het vormgeven van de strategische richting van de organisatie, waarbij informatiebeveiliging is geïntegreerd in de besluitvorming en bedrijfsprocessen. De CISO zorgt ervoor dat het beleid en de strategieën voor informatiebeveiliging aansluiten bij de bedrijfsdoelen en risicobereidheid van de organisatie, en rapporteert periodiek aan het bestuur over de status en voortgang van de informatiebeveiligingsinitiatieven.

PROFIEL
De functie vereist het voortdurend balanceren van tegenstrijdige belangen tussen business, IT, compliance en externe toezichthouders. Beslissingen worden soms genomen met beperkte informatie, waarbij de impact direct voelbaar kan zijn op de continuïteit, reputatie en compliance van CZ. De CISO moet in staat zijn om complexe beveiligingsvraagstukken te vertalen naar strategische keuzes en concrete maatregelen die breed gedragen worden binnen de organisatie. Daarom adviseert de CISO, hoewel operationeel gelieerd aan de divisie Data & IT, direct in een functionele lijn aan het bestuur en de Raad van Commissarissen, om objectief inzicht te bieden in de IT-risico's en de bredere cyberweerbaarheid. Waar strategische voorstellen en besluiten worden voorgelegd aan en afgestemd met het bestuur, zodat zij hierin hun verantwoordelijkheid kunnen nemen. In het geval van een significante dreiging of security incident, waarin snel en adequaat handelen is vereist, heeft de CISO het mandaat om organisatiebrede maatregelen af te dwingen in het directe belang van CZ. De CISO weet complexe materie eenvoudig uit te leggen, anticipeert op toekomstige ontwikkelingen en vertaalt trends in de buitenwereld naar intern securitybeleid.

Je beschikt over:
- WO werk- en denkniveau; heeft een goed ontwikkeld abstraherend en analytisch vermogen.
- Ervaring (minimaal 10 jaar) op een gelijkwaardig niveau binnen het vakgebied van informatiebeveiliging.
- Relevante certificering op het vakgebied security en informatiebeveiliging (CISSP, CISM, CRISC).
- Kennis van wet- en regelgeving ten aanzien van Informatiebeveiliging.
- Kennis van relevante marktontwikkelingen en bedreigingen ten aanzien van Informatiebeveiliging.
- Netwerk onderhouden op het vakgebied, bijvoorbeeld door lidmaatschap van vakverenigingen of het initiëren van kennisuitwisseling met verzekeraars in de branche.

Daarnaast beschik je over de volgende competenties:
- Ervaring in het adviseren van het bestuur over strategische beveiligingsvraagstukken.
- Vermogen om als strategisch partner op te treden en samen te werken met senior management en andere belanghebbenden.
- Ervaring met het wegen van tegenstrijdige belangen en prioriteringsvraagstukken.
- In staat om complexe beveiligingsinformatie te vertalen naar strategische aanbevelingen en actieplannen.
- Sterke sociale en communicatieve vaardigheden.

- Overige kenmerken: integer, proactief, stressbestendig, zelfsturend, samenwerkingsgericht, resultaatgericht, standvastig.

ARBEIDSVOORWAARDEN
CZ biedt je een uitdagende functie in een prachtig bedrijf met een fijne cultuur, waarin je veel impact kunt maken en waarmee je direct een maatschappelijke bijdrage kunt leveren om het digitale leven van haar klanten en bezoekers positief te beïnvloeden. En niet te vergeten, er is veel ruimte voor zelfontwikkeling door middel van uitgebreide opleiding- en ontwikkelmogelijkheden.
Je komt te werken in een veelzijdige omgeving, met een open en moderne cultuur, een goede werksfeer waar collega's nauw samenwerken, elkaar prikkelen én ondersteunen.
Naast het bovenstaande mag je rekenen op:

- Een fulltime functie, waarbij deels thuis en flexibel werken de normaalste zaak van de wereld is;
- Een marktconform maandsalaris met een bijpassende inschaling tot maximaal van €10.342,00 afhankelijk van opleiding, kennis en werkervaring.
- Vakantiegeld en 13^{e} maand;
- 28 vakantiedagen op jaarbasis;
- Een passende reiskostenregeling;
- Een uitstekende pensioenregeling met een lage eigen bijdrage;
- Uiteraard krijg je de beschikking over een laptop en een mobiele telefoon;
- Diverse faciliteiten en mogelijkheden, waaronder korting op CZ-producten.

PROCEDURE
De wervings- en selectieprocedure wordt uitgevoerd door InterExcellent. Op basis van de brief en cv-selectie worden kandidaten uitgenodigd voor een oriënterend gesprek met InterExcellent. De meest passende kandidaten worden daarna voorgedragen aan de selectiecommissie bij CZ die beslist met wie zij wenst kennis te maken. Van de eindkandidaten kunnen referenties worden nagetrokken. Een (ontwikkel)assessment maakt onderdeel uit van de procedure.

SOLLICITEREN EN PLANNING
Ben jij de daadkrachtige, inspirerende en verbindende CISO die strategisch leiderschap toont op het gebied van digitale operationele weerbaarheid? Ben je een veranderaar die wil bouwen en impact wil maken? En herken jij jezelf in het profiel? Dan zien we jouw sollicitatie graag tegemoet.
Sollicitaties (een functiegerichte motivatiebrief plus CV) ontvangen we graag zo spoedig mogelijk, via InterExcellent.

CONTACT OVER DEZE VACATURE
Deze procedure wordt uitgevoerd door Sietse Bergstra, Managing Partner, en Riëtte Coolen, Senior IT Recruitment Consultant, InterExcellent IT Regie Management, Baarn. Tel: 035 - 5280430, www.interexcellent.nl

We zien met belangstelling uit naar je reactie en/of sollicitatie!