Interview met Hermen Koole

Implementatie DORA bij OpGroen Verzekeringen

OpGroen, voorheen onderdeel van Aon, is sinds 1 augustus 2024 een zelfstandig verzekeringsadvies- en volmachtbedrijf in Nederland. OpGroen biedt een breed scala aan particuliere verzekeringen en diensten, waaronder autoverzekeringen, reisverzekeringen en inboedelverzekeringen.

Hoe zijn jullie bij InAudit terecht gekomen?
Wij hebben eerder goede ervaringen opgedaan met InAudit op het gebied van ondersteuning bij compliance vraagstukken. Vanuit deze ervaring hebben we InAudit nu in eerste instantie gevraagd om een onafhankelijke DORA gap-analyse. In tweede instantie hebben we het verzoek uitgebreid met de vraag om ons interne DORA projectteam te ondersteunen met onder andere project aanpak, inbreng kennis en capaciteit.

Waarom is DORA belangrijk voor OpGroen?
Bij OpGroen hebben we de Digital Operational Resilience Act (DORA) geïmplementeerd om onze digitale veerkracht en cybersecurity te versterken. DORA stelt eisen aan de operationele veerkracht van financiële instellingen en zorgt ervoor dat wij in staat zijn om IT-gerelateerde bedreigingen te weerstaan, erop te reageren en ervan te herstellen.

Onze aanpak omvat een gedetailleerde roadmap en een focus op kritieke derde partijen, systeemmapping en incidentrespons. Door DORA te implementeren, verhogen we de veiligheid en betrouwbaarheid van onze diensten, wat bijdraagt aan het vertrouwen van onze klanten en partners.

Hoe kijk je naar DORA, hard nodig of bureaucratische regels?
Met de toegenomen digitalisering is er meer afhankelijk van IT. De grote omvang van steeds globaler opererende IT-leveranciers en het grote aandeel dat deze leveranciers hebben op de kwaliteit in de hele financiële sector maakt regulering belangrijk. Inzicht hebben in belangrijke spelers in de hele keten en eventuele kwetsbaarheden daarin zoveel mogelijk beperken, helpt ons allemaal. Kortom, het is goed om met Europese regelgeving en de sector deze kwetsbaarheden aan te pakken.

Naam: Hermen Koole
Functie: CFO
Bedrijf: OpGroen Verzekeringen
Achtergrond: Hermen Koole is sinds vorig jaar CFO bij OpGroen Verzekeringen. Hij heeft een achtergrond als accountant en is de afgelopen 20 jaar voornamelijk werkzaam geweest in de financiële sector.

Wat is de belangrijkste impact van DORA?
Op korte termijn betekent het voor OpGroen vergroting van de bewustwording van informatiebeveiligingsrisico's en dat we interne procedures en vastlegging van beheersingsmaatregelen hebben aangescherpt. De effectieve werking van de beheersingsmaatregelen zal gevolgd en waar nodig verbeterd worden. Daarnaast is het proces voor incidentmelding voorbereid en geoefend. Ook zijn we gestart met het reviewen en bespreken van de contracten met IT-leveranciers zodat ze voldoen aan de DORA vereisten. Op de midden- en lange termijn verwacht ik dat het niveau van informatiebeveiliging in de hele verzekeringsketen verbetert.

DORA vereist dat financiële entiteiten hun keten aan IT-dienstverleners beheersen. Is dat een reële verplichting?
Deze verplichting wordt meer haalbaar mede dankzij de invoering van Europese wetgeving zoals onder andere DORA. De gezamenlijke kracht van wetgeving, toezicht en de vraag vanuit de financiële sector aan de IT-dienstverleners zal bijdragen aan verbeterde beheersing van de informatiebeveiliging in de hele keten.

Hoe vullen jullie het raamwerk voor informatiebeveiliging in?
Voor het informatiebeveiligingsbeleid hanteren we nu zoveel mogelijk het ISO27001 raamwerk. De DORA vereisten passen we hierin.

Er is van alles in beweging op IT vlak met ransomware, AI, social media, maar ook geopolitieke ontwikkelingen. Waar maak jij je het meest zorgen over?
De geopolitieke ontwikkelingen en daarmee een grotere oorlogsdreiging, vergroten mijn generieke zorgen als het gaat om kwetsbaarheden in ons leven door de afhankelijkheid van IT. Maar ook los van de vraag of kwetsbaarheden in IT worden misbruikt door overheden voor digitale oorlogsvoering vind ik dat we het beschermen tegen deze risico's de hoogste prioriteit moeten geven. Daarmee beperken we de mogelijkheden voor iedereen die kwaad wil.

Hoe zorg je als bestuurder dat de informatiebeveiliging in control is?
Het begint bij collega's met interesse, kennis en een lerende organisatiecultuur waarin risicobewustzijn wordt gestimuleerd. Vervolgens zijn natuurlijk een gedegen risicoanalyse, een goed informatiebeveiligingsbeleid en het bewaken van de werking van de beheersmaatregelen van groot belang. Het vraagt discipline om continu te blijven evalueren en ontwikkelen maar het resultaat is van onschatbare waarde.

Hoe verwacht je dat de AFM als toezichthouder zijn rol gaat invullen?
Ik ben positief over de betrokkenheid en informatievoorziening vanuit de AFM in de aanloop naar de invoering van DORA. Hoe de AFM haar rol gaat invullen is natuurlijk niet aan mij om te beantwoorden. Ik kan alleen maar aangeven dat ik verwacht dat de AFM constructief kritisch en streng maar rechtvaardig haar rol zal invullen.

Betekent DORA ook dat je nu 's nachts beter slaapt (omdat de IT-risico's beter worden beheerst)?
Het draagt er in ieder geval wel aan bij ;-).

OpGroen

www.opgroen.nl