Een keten is zo sterk als de zwakste schakel

NATASCHA VAN DUUREN
DE CLERCQ

Natascha van Duuren benadrukt dat cybersecurity al lang niet meer alleen gaat om technologie. Het gaat ook om kennis en bewustwording bij medewerkers, in alle lagen van de organisatie, inclusief bij bestuurders. Evenals het vermogen van een organisatie om aantoonbaar security risico's te managen. Dit betekent dat beveiligingsmaatregelen vastgelegd moeten worden in beleid, onderbouwd met risicoanalyses, vastgesteld op managementniveau en ingebed in een Plan-Do-Act-Check-cyclus.

De regelgeving op het gebied van cybersecurity wordt veelomvattender en strenger. Het is voor ondernemingen niet eenvoudig alle wettelijke eisen in kaart te brengen en de impact daarvan op waarde te schatten. Het is volgens Natascha van Duuren bijvoorbeeld onontbeerlijk de gehele keten van toeleveranciers in beeld te hebben. Waar in de keten zitten eventuele risico's? Welke contractuele afspraken kunnen met toeleveranciers worden gemaakt om cybersecurityrisico's in de keten zo klein mogelijk te maken? Een keten is immers zo sterk als de zwakste schakel.

Als organisaties onverhoopt toch getroffen worden door een incident, dan is het van belang dat zij onmiddellijk een beroep kunnen doen op experts die hen adviseren en bijstaan bij de afhandeling van het incident. Daar komt veel bij kijken en dat vereist specialistische kennis. Zo dient er bijvoorbeeld zo snel mogelijk zicht te komen op de omvang van het incident, moeten wettelijke meldplichten tijdig worden nageleefd, moet geïnventariseerd worden welke effecten het incident op contractuele afspraken met derden heeft, dient de communicatie intern en extern consistent te zijn en zal onderzocht moeten worden of en hoe de schade kan worden verhaald op derde partijen. Bij dit alles is snelheid en deskundigheid vereist. De Clercq beschikt over een groot netwerk met forensisch IT-specialisten en andere adviseurs waarmee zij korte lijnen heeft en snel kan schakelen.

'De Clercq beschikt over een groot netwerk met forensisch IT-specialisten en andere adviseurs waarmee zij korte lijnen heeft en snel kan schakelen'

Veel ondernemingen zijn helaas nog onvoldoende op de hoogte van de cyberdreigingen waar zij mee te maken hebben en de wet- en regelgeving die op hen afkomt, zo constateert Natascha van Duuren. Terwijl dit van groot belang is. Zo stelt de nieuwe NIS2 Richtlijn strengere eisen aan maatregelen voor het beheer van cybersecurityrisico's, dienen deze maatregelen te worden goedgekeurd door de bestuurder, dient de bestuurder toe te zien op de naleving van deze maatregelen en kan de bestuurder – bij gebreke daarvan – zelfs persoonlijk aansprakelijk worden gesteld. De voornaamste drijfveer voor bestuurders om de risico's van cyberincidenten (het liefst proactief) zo veel mogelijk te beperken zou volgens Natascha van Duuren echter niet de dreiging van boetes moeten zijn, maar de exponentiële groei van cyberaanvallen. Volgens cybersecurity experts is het einde helaas nog niet in zicht zodat cybersecurity prioriteit één van boardrooms moet zijn en blijven.