Ceo heeft eigen aansprakelijkheid cybersecurity niet op het netvlies

- Te veel bedrijven blijven tekortschieten als het gaat om de veiligheid van hun IT-systemen.
- De eisen op het gebied van cybersecurity worden daarom door Brussel fors aangescherpt.
- Bedrijfsbestuurders zijn zich te weinig bewust van hun eigen aansprakelijkheid op dit vlak.

Sandra Olsthoorn en Ardi Vleugels
Amsterdam

Bestuurders van bedrijven zijn zich onvoldoende bewust van de risico's die zij volgend jaar lopen. Europese regels die dan ingaan, maken hen expliciet verantwoordelijk voor het cyberbeleid van hun onderneming. Ze kunnen persoonlijk aansprakelijk worden gesteld als ze deze taak niet goed vervullen en kunnen in het uiterste geval zelfs tijdelijk uit hun functie worden gezet.

Daarvoor waarschuwt de Cyber Security Raad (CSR), die de overheid adviseert over digitale veiligheid. Tot nu toe lieten bestuurders cyberbeleid vaak over aan IT-afdelingen en was hun rol beperkt tot het goedkeuren van het gevraagde budget. In de nieuwe Europese regels, die voor veel bedrijven gaan gelden en die op dit moment naar Nederlandse wetgeving worden vertaald, moeten ze meer doen.

De CSR ziet dat veel bedrijven dit niet doorhebben. Zo moeten bestuurders maatregelen tegen cyberrisico's goedkeuren en toezien op uitvoering. Ook moeten ze meehelpen om de cybersecurity bij directe toeleveranciers te waarborgen.

Advocaat en hoogleraar Lokke Moerel, lid van de raad, noemt de regels revolutionair omdat bestuurders zo nadrukkelijk worden aangesproken op hun verantwoordelijkheden. 'Als je die negeert, zal sneller sprake zijn van een ernstig persoonlijk verwijt, waardoor persoonlijke aansprakelijkheid van bestuurders op de loer ligt. Dit strekt zich zelfs uit tot de commissarissen.'

In eerste instantie krijgt een nalatig bedrijf waarschuwingen en boetes, tot 2% van de jaaromzet. Als daarna voldoende verbetering uitblijft, kan een bestuurder persoonlijk gevolgen ondervinden. 'Die moet dus snel zijn kennis oppoetsen en controleren hoe het bedrijf er voorstaat', zegt Moerel.

Nu bedrijven digitaal sterk verbonden zijn, kan een zwakke achterdeur bij een kleine leverancier voor de hele keten gevolgen hebben. De nieuwe regels dwingen grote bedrijven daarom meer verantwoordelijkheid te nemen voor hun toeleveranciers. Ze moeten hen helpen, bijvoorbeeld door hun kennis te delen.

Wat betreft cyberveilig werken blijven juist kleinere bedrijven achter, zegt CSR-lid Claudia de Andrade, bij Havenbedrijf Rotterdam verantwoordelijk voor de IT. 'Naar schatting 60% van de grotere en 30% van de kleinere bedrijven is zich bewust van cyberrisico's.' Uit een uitvraag van cybersecuritybedrijf Cisco bleek vorige week dat maar 3% van alle bedrijven klaar is voor actuele cyberdreigingen.

'Wetgevers hebben gedacht: nou dan máken we van cybersecurity wel chefsache'

In Nederland gaan de regels per 2025 in, maar de inhoud is al grotendeels bekend en zal niet meer veranderen, denkt de raad. 'Om de invoeringsdatum te halen moet je nu beginnen', zegt Hester Somsen, directeur cybersecurity en statelijke dreigingen bij de NCTV. 'Regel je opleidingen, ga aan de slag met een risicoanalyse. Doe je dat niet, dan ben je kwetsbaar voor cyberaanvallen en uiteindelijk nalatig.'

Een deel van de regels, zoals een meldplicht bij cyberincidenten, geldt nu al voor zo'n duizend essentiële bedrijven, zoals in de telecom. Met de nieuwe wet zullen zo'n 10.000 bedrijven ermee te maken krijgen.

Moerel: 'Ook sectoren zoals de voedselproductie gaan straks voor het eerst onder een toezichthouder vallen voor hun cyberbeleid.' Dat besef is er niet bij iedereen: regelmatig ziet zij bedrijven die schrikken omdat ze nu pas ontdekken dat ook zij onder de regels gaan vallen. Met onlinetests kunnen bedrijven nagaan wat ze moeten doen.

Overheid en experts roepen al jaren op de bewaking tegen cyberaanvallen te verstevigen, maar veel bedrijven namen een laconieke houding aan. Dat bestuurders nu expliciet verantwoordelijk worden, is een zwaar middel, maar daarom logisch, vindt Moerel. 'Wetgevers hebben gedacht: nou dan máken we het chefsache.'

De strenge regels komen er niet voor niets: de risico's van cyberincidenten waren nooit eerder zo groot, stelt de CSR. Ransomware kan de bedrijfsvoering stilleggen en door spanningen in de wereld loopt de digitale dreiging fors op. Het aantal aanvallen neemt toe, mede door kunstmatige intelligentie. Moerel: 'Cyberincidenten staan in de top drie van grootste bedrijfsrisico's.'

Somsen wijst erop dat een cyberaanval op een bedrijf ook maatschappijontwrichtend kan zijn. 'Nederland heeft dat op die schaal nog niet gezien. Maar wij achten dat risico hier meer dan reëel.' Moerel: 'Zoals we er nu voorstaan, zijn we daar qua cyberweerbaarheid niet klaar voor.'