‘Retail moet rekening houden met meer cyberaanvallen’

08-07-2014 07:08

Bestuursleden van concerns hebben te weinig oog voor de gevaren van cybercriminaliteit. Dat zegt bestuursadviseur Dick Berlijn van adviesbureau Deloitte in het Financieele Dagblad. Waar banken ‘hun lesje hebben geleerd’, richten criminelen zich op ondernemingen waar het gevoel van urgentie te wensen overlaat, stelt hij op basis van onderzoek van Deloitte.

Berlijn signaleert bij raden van bestuur een gebrek aan bewustzijn als het gaat om de risico’s van onvoldoende beveiligde netwerken. Daarnaast spelen de kosten van een verbeterde cyberveiligheid een rol. “Maar als het dan een keer fout gaat, en dat gaat het altijd een keer, kunnen de gevolgen ingrijpend zijn. Langzamerhand ook voor bestuurders persoonlijk.”

Ceo Gregg Steinhafel vertrok bijvoorbeeld bij de Amerikaanse winkelketen Target nadat cybercriminelen informatie hadden gestolen van miljoenen credit- en betaalkaarten van klanten. Steinhafel erkende later dat de keten waarschuwingssignalen niet tijdig had herkend.

Zowel fysieke als online retailers staan meer cyberaanvallen te wachten, stelt hij. “Voor een retailbedrijf is het bedrijfsmatig zeer bedreigend als de logistieke processen stil komen te liggen”, geeft Berlijn als voorbeeld van mogelijke risico’s. Om de veiligheid te verhogen is volgens hem inzicht nodig in wat beveiligd moet worden en hoe een aanval kan worden ontmanteld.

Daarnaast is het belangrijk om te weten welke mogelijke partijen een cyberaanval kunnen uitvoeren en wat criminelen daarbij willen bemachtigen. “Kennis van de vijand, zijn middelen en motivaties is de eerste stap om beslissingen te nemen over adequate bescherming”, aldus Berlijn.

In 2013 vonden wereldwijd in totaal 47.479 cybercrime-incidenten plaats. Daarvan deden zich er 467 voor binnen de detailhandel, blijkt uit onderzoek van telecombedrijf Verizon. Het ontoegankelijk maken van websites kwam met 33 procent het vaakst voor, gevolgd door invallen in virtuele kassa’s (31 procent). Daarnaast vallen cybercriminelen websites van retailers aan (tien procent) en worden betaalpassen geskimd (zes procent). In vier procent van de gevallen komt misbruik door insiders voor. Bij twee procent gaat het om verlies of diefstal door een fout of onoplettendheid of kwaadaardige software. Cyberspionage komt met minder dan een procent het minst vaak voor.