CHEFSACHE

Bestuurders aansprakelijk na ernstige cyberaanval

Axel Arnbak

Al jaren lezen wij in de krant dat cybersecurity een groeiend maatschappelijk probleem is. Maar of de toenemende zorgen organisaties daadwerkelijk aanzetten tot actie bleef lang de vraag. Het antwoord wordt steeds duidelijker. Handhavingsboetes bij ernstige datalekken kunnen onder de nieuwe Europese datawetgeving oplopen tot 4% van de wereldwijde jaaromzet. Bovendien kunnen bestuurders persoonlijk aansprakelijk gesteld worden bij ernstige cyberaanvallen, en zijn de eerste schadeclaims al een feit. Cyberaanvallen kunnen zowel ondernemingen als individuele bestuurders diep in de portemonnee raken. Cybersecurity is chefsache.

Gregg Steinhafel stapte in mei 2015 op als ceo van de Amerikaanse retailer Target, na een creditcard-hack vlak voor kerst. Target moest de klanten een persoonlijke e-mail sturen en liep miljoenen mis omdat zij hun kerstinkopen vervolgens bij de concurrent deden. Later bleek de hack niet een kleine subgroep maar 70 miljoen klanten te hebben getroffen. Target had dit verzwegen. De koers kelderde, exit Steinhafel.

Door een zware hack in 2011 bij de kleine Beverwijkse certificatenaanbieder Diginotar lag het Nederlandse internet een week plat, vooral in de publieke sector. Daarop ging Diginotar vrij snel failliet. Kort voor de hack was Diginotar overgenomen. De nieuwe eigenaar wist in 2014 met succes bij de rechtbank Amsterdam de vorige bestuurders aansprakelijk te stellen, omdat zij de zwakke beveiliging hadden verzwegen voor de kopers. Via hun persoonlijke bv's moesten zij miljoenen euro's terugbetalen. Amerikaanse toestanden in de polder.

Sinds 1 januari 2016 heeft de wetgever bestuurdersaansprakelijkheid expliciet mogelijk gemaakt bij ernstige datalekken. Niet alleen een instructie tot onrechtmatig handelen kan daartoe leiden, ook het laten voortduren ervan of nalaten van preventieve maatregelen te treffen. Momenteel behandelt het parlement een meldplicht beveiligingsincidenten in brede zin, of er nu een datalek is of niet. Een cyberaanval die de energievoorziening, gezondheidszorg of het financiële verkeer lamlegt, leidt dan meteen tot vragen van toezicht- en aandeelhouders. Als blijkt dat een organisatie willens en wetens verouderde of verzwakte IT-systemen gebruikt, lopen onderneming en bestuurder een serieus risico. Vooral als het bestuur na interne escalatie pijnlijke feiten verzwijgt of verdraait om onder de radar te blijven.

Target en Diginotar tonen hoe cyberaanval grote en kleine onderneming diep in de problemen brengt

Niet alleen de media en IT-consultants, zelfs conventionele juridische vaktijdschriften publiceren nu over aansprakelijkheid bij cyberaanvallen. Vorige week verscheen een sterk overzichtsartikel van Eric Tjong Tjin Tai. De Tilburgse hoogleraar privaatrecht is alleen wat te voorzichtig waar hij vermoedt dat de schade na een datalek meevalt. Target en Diginotar tonen hoe een cyberaanval een grote en kleine onderneming diep in de problemen brengt of zelfs de nek omdraait, met miljoenenschade als gevolg.

Daarnaast breidt de nieuwe Nederlandse datawetgeving de handhavingsboetes uit tot maximaal 10% van de binnenlandse jaaromzet. De nieuwe EU-wet, die per mei 2018 de Nederlandse vervangt, maximeert de boete op 4% van de mondiale jaaromzet. Legt een toezichthouder zo'n heftige boete op, dan is er echt iets goed misgegaan en zullen aandeelhouders niet terugdeinzen hun schade op een bestuurder te verhalen. De EU-wet bevat ook een nieuw regime voor 'class action'-procedures. Net als in de financiële sector kunnen opportunistische stichtingen beperkte individuele dataschade gezamenlijk ophalen bij de rechter. Via internet zijn duizenden klanten van een groot bedrijf zo gevonden. De naderende beveiligingsnachtmerrie van het internet der dingen doet nog een flinke duit in het zakje. Zie als bestuurder een 'connected' cv-ketel, auto of televisie een jaar na aankoop maar beveiligd te houden tegen cyberaanvallen.

Beveiliging blijft moeilijk, maar bestuurders kunnen zich niet meer verschuilen achter de cybercomplexiteit. Vooral verdraaien en verzwijgen zal hard aangepakt worden. Verzekeraars houden hun beurzen dan gesloten. Als cybersecurity vanuit maatschappelijk oogpunt nog geen boardroom-issue was, zal de trend richting hoge boetes en bestuurdersaansprakelijk na ernstige cyberincidenten daarin het sluitstuk vormen.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: **@axelarnbak**