VANIERSEL LUCHTMAN ADVOCATEN

VAST | VERZEKERINGSRECHT AANSPRAKELIJKHEID SCHADE EN TOEZICHT

Dit artikel is verschenen in en geschreven voor het tijdschrift VAST. Het artikel is met veel aandacht en zorgvuldigheid geschreven, maar bevat informatie van algemene aard. Juridisch advies is echter altijd maatwerk. Wint u dus altijd deskundig juridisch advies in. (Lees onze disclaimer).

VAST 2021, B-047, Thom Broer, e-ISSN 2667-307X, M.A.D. Lex, vast-online

IT-serviceverlener aansprakelijk voor deel van de schade na ransomsoftware-blokkade

26 oktober 2021

Steeds meer bedrijven zijn actief bezig met het digitaliseren van de bedrijfsvoering. De coronapandemie zorgde voor een golf aan thuiswerkers, waardoor bedrijven zich genoodzaakt zagen om snel hun hele bedrijfsvoering hierop aan te passen. Dit brengt kansen met zich mee, maar ook gevaren. Hackers zijn dit jaar extra actief en richten zich niet enkel op grote bedrijven. Ook kleine bedrijven lopen het risico om slachtoffer te worden van cyberaanvallen. Hierna ga ik in op de ontwikkelingen op het gebied van het verzekeren tegen cyberaanvallen en een in dat kader relevante recente aansprakelijkheidszaak bij het gerechtshof Amsterdam.

Verzekeren tegen cyberaanvallen

Recent verscheen op BNR een artikel over het feit dat het steeds moeilijker wordt voor bedrijven om zich te verzekeren tegen cyberaanvallen. Verzekeraars sluiten hele sectoren uit of stellen limieten aan de omzet. Bedrijven die aan het groeien zijn, worden soms overvallen met premies die met 50 tot soms wel 800 procent gestegen zijn. Voor veel bedrijven zullen dergelijke stijgingen niet betaalbaar zijn, waardoor verzekeren geen optie meer is. Voor de bedrijven die de premies nog wel kunnen betalen, wordt de dekking vaak ingeperkt.

Door deze beperkte dekking komt de nadruk te liggen op een goed geregelde IT-afdeling. Bedrijven kunnen zelf IT'ers in dienst nemen, maar ook overeenkomsten sluiten met gespecialiseerde dienstverleners. In de praktijk maken kleine bedrijven vaak gebruik van de laatstgenoemde optie. Hierdoor verschuift een deel van het risico naar deze dienstverlener, waardoor de ondernemer zich minder zorgen hoeft te maken over het beheer en onderhoud van zijn ICT-systeem.

Aansprakelijkheid IT-serviceverlener

Vaak ziet een overeenkomst tussen een bedrijf en IT-serviceverlener (hierna: 'IT'er') op het beheer en onderhoud van het ICT-systeem. De exacte inhoud en omvang van een dergelijke overeenkomst hangt af van de afspraken die worden gemaakt, maar over het algemeen ziet het minimaal op het werkzaam en up-to-date houden van het ICT-systeem. Ook wordt vaak een back-upsysteem opgezet, zodat regelmatig (het liefst dagelijks) een back-up wordt gemaakt. Mocht het bedrijf getroffen worden door een cyberaanval, dan kan deze back-up worden teruggezet en de bedrijfsvoering doorgaan (tenzij de back-up ook gegijzeld is). De ondernemer kan zich dan focussen op de bedrijfsvoering en bij problemen contact opnemen met de IT'er.

In een uitspraak van het gerechtshof Amsterdam van 16 februari 2021 was de bijzondere situatie ontstaan dat de ondernemer (hierna: 'Drenth') de overeenkomst met de IT'er (hierna: 'Bultsma') had opgezegd per 21 juni 2016. De overeenkomst met de nieuwe IT'er (hierna: 'Biesenbeek') ging pas in op 1 augustus 2016. In de periode tussen 21 juni 2016 en 1 augustus 2016 was Drenth dus niet beschermd. En u raadt het al, op 19 juli 2016 wordt Drenth getroffen door een ransomsoftware-blokkade. Drenth heeft vervolgens geprobeerd om een back-up terug te zetten, maar constateerde dat sinds 2013 geen back-ups waren gemaakt, met uitzondering van een zeer beperkt handmatige back-up van 29 april 2016. Nu Drenth geen overeenkomst meer had met Bultsma en Biesenbeek pas vanaf 1 augustus zou starten, zat hij met een probleem. Drenth heeft vervolgens losgeld betaald en op 29 juli 2016 is het ICT-systeem weer opgestart en gecontroleerd.

Drenth stelt dat Bultsma toerekenbaar is tekortgeschoten in de nakoming van haar verplichtingen uit de overeenkomst, nu zij geen goede (en recente) back-ups heeft gemaakt van het ICT-systeem. Drenth spreekt Bultsma daarom aan voor de geleden schade, te weten € 17.262,27. Dit bedrag ziet voornamelijk op het opzetten van noodsystemen, betaling van het losgeld, beperken van de schade en het feit dat het bedrijf drie dagen stillag. Bultsma stelt dat zij niet aansprakelijk is, omdat er een werkbare back-up van 29 april 2016 beschikbaar was. Tevens stelt Bultsma dat de overeenkomst per 21 juni 2016 was beëindigd en het beheer van het ICT-systeem niet meer bij haar lag. Verder liep Biesenbeek al vanaf maart 2016 mee bij Drenth en heeft zij in die periode nieuwe servers geïnstalleerd en waarschijnlijk wijzigingen aangebracht in het oude systeem.

Het hof overweegt dat Bultsma tot 21 juni 2016 verantwoordelijk was voor het beheer- en onderhoud van het ICT-systeem. Deze verantwoordelijkheid hield onder andere in dat er een volledige back-up van het systeem tot 21 juni 2016 beschikbaar had moeten zijn. Het feit dat Biesenbeek al meeliep vanaf maart 2016 doet hier verder niets aan af. Desondanks acht het hof Bultsma niet verantwoordelijk voor alle schade. Het hof overweegt dat Drenth zelf ervoor heeft gekozen om de overeenkomst met Biesenbeek pas op 1 augustus 2016 in te laten gaan. Ook indien een back-up van 21 juni 2016 aanwezig was geweest, had Drenth enige schade geleden die in dat geval geheel aan haar zou zijn toe te rekenen. Het hof overweegt dat twee derde van de door Drenth geleden schade het gevolg is van feiten en omstandigheden die aan haarzelf kunnen worden toegerekend.

Het hof overweegt dat Bultsma aansprakelijk is voor een derde van de geleden schade en veroordeelt haar tot betaling van € 5.754,09 aan schadevergoeding. Bultsma moet tevens de onderzoekskosten van een ingeschakelde IT-deskundige betalen (€ 2.011,63) en de proceskosten in beide instanties (€ 6.614,42).

Gedeelde verantwoordelijkheid

Uit deze uitspraak blijkt dat zowel de IT'er als de ondernemer een verantwoordelijkheid hebben wat betreft het beheer en onderhoud van het ICT-systeem. Het feit dat de opvolgende IT'er al meeloopt bij de onderneming, zorgt niet voor een verschuiving van de verantwoordelijkheid. Tot de einddatum van de overeenkomst is de oude IT'er verantwoordelijk voor de uitvoer van het beheer en onderhoud van het ICT-systeem.

Daaronder valt tevens het verzorgen van een degelijke en recente back-up. Daarnaast moet de ondernemer echter bewust zijn van het feit dat zijn bedrijf gevaar loopt als hij geen overeenkomst heeft met een IT'er. De ondernemer kan dit risico niet zomaar afschuiven op een ander.

Hoewel een IT'er niet altijd kan beletten dat een cyberaanval plaatsvindt, geldt hier toch het gezegde: beter voorkomen dan genezen. Zeker met de stijgende verzekeringspremies kan een goede cybersecurity het verschil maken. Ondernemers doen er dus goed aan om actief samen te werken met hun IT'er en te zorgen dat simpele zaken zoals het maken van back-ups en up-to-date houden van antivirus software goed geregeld zijn.