Naam Annemarie Bolscher
Functie advocaat
Organisatie Louwers
IP|Technology Advocaten

IT-LEVERANCIER MOET ZORGEN VOOR ADEQUATE BEVEILIGING

LEVERANCIERS AANSPRAKELIJK BIJ CYBERAANVALLEN

Aanvallen met ransomware nemen toe. Dé vraag hierbij is of er recente back-ups zijn. IT-advocaat Annemarie Bolscher bespreekt rechtelijke uitspraken over de aansprakelijkheid van klant en IT-leverancier en geeft concrete tips.

Cybercrime is steeds vaker prominent in het nieuws. Organisaties lijden schade doordat hun IT-netwerk wordt gehackt. Zij betalen vaak forse bedragen om weer toegang te krijgen tot hun netwerk en gegevens. Vaak blijkt pas tijdens een hack dat de gemaakte back-ups ontoereikend zijn. Regelmatig worden IT-leveranciers hiervoor aansprakelijk gesteld, maar dit betekent niet altijd dat alle schade kan worden verhaald.

Cyberbeveiliging
Cybersecurity is door de Europese Commissie (EC) bestempeld als een van de kernelementen van haar digitale strategie. In 2019 is de Cyberbeveiligingsverordening in werking getreden, die een Europees kader introduceert voor cyberbeveiligingscertificering van ICT-producten, -diensten, en -processen. De verordening wordt in Nederland uitgevoerd met de Uitvoeringswet Cyberbeveiligingsverordening. Dit is nu nog een wetsvoorstel dat onder meer de aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit regelt. In Nederland zal het Agentschap Telecom de taken uitvoeren. Daarnaast wordt in het wetsvoorstel de verstrekking van bepaalde Europese cyberbeveiligingscertificaten geregeld, en een kader in het leven geroepen voor handhaving en toezicht. Certificering is voor IT-leveranciers in principe vrijwillig, maar de EC zal voor het einde van 2023 aangeven of bepaalde certificeringsschema's alsnog verplicht worden.

Topprioriteit
Dit alles zal hopelijk bijdragen aan een betere beveiliging van software. Bedrijven en instellingen zullen echter zelf ook van de beveiliging van hun netwerk een topprioriteit moeten maken. De Autoriteit Persoonsgegevens kan fikse boetes opleggen in geval van een (dreigend) datalek. Tot eind 2020 zijn 12 boetes opgelegd. De openbaar gemaakte boetes varieerden van 12.000 tot 830.000 euro. Maar los daarvan kan de schade natuurlijk aanzienlijk zijn als kostbare data verloren gaat. Uit de rechtspraak blijkt dat het regelmatig gebeurt dat partijen geen afspraken maken over de beveiliging van hun

“Schade bleef deels voor de afnemer, omdat die alleen simpele wachtwoorden wilde gebruiken”

IT-netwerken en ook niet over het veiligstellen van data door middel van back-ups. De gangbare opvatting in de rechtspraak is dat op een IT-leverancier geen algemene verplichting rust om een back-up te maken van alle volledige bestanden van de klant. Recent zijn wel uitspraken gepubliceerd waarin de IT-leverancier aansprakelijk werd gehouden voor de schade naar aanleiding van een ransomware-aanval. Toch bleef toen een deel van de schade voor rekening van de afnemer.

Verantwoordelijkheid

De rechtbank Amsterdam hield een IT-leverancier verantwoordelijk voor inadequate beveiligingsmaatregelen, terwijl partijen hierover geen schriftelijke afspraken hadden gemaakt. Het geschil ging over een administratiekantoor dat aan een IT-leverancier de (mondelinge) opdracht had gegeven tot herinrichting van zijn IT-infrastructuur. Op enig moment werd het netwerk van het administratiekantoor gehackt. Alle bestanden op de server werden versleuteld, waaronder de back-ups. Na betaling van 3 bitcoins van 963,61 euro per stuk kreeg het kantoor weer toegang tot de bestanden.

Nader onderzoek wees uit dat bij het administratiekantoor onder meer een firewall ontbrak, dat de back-upvoorzieningen niet goed waren ingeregeld en dat sprake was van zwakke wachtwoorden. Het administratiekantoor stelde de IT-leverancier aansprakelijk voor de schade, omdat het meende dat het zijn IT-infrastructuur volledig in handen had gelegd van de leverancier en dat de beveiliging daar vanzelfsprekend ook bij hoorde. De leverancier gaf aan dat hij wel beveiligingsmaatregelen had voorgesteld, maar dat de afnemer die te duur vond.

Adequate beveiliging

De rechtbank oordeelde dat de IT-leverancier had moeten zorgdragen voor een adequate beveiliging. Het feit dat het administratiekantoor daaraan niet wilde meewerken, deed daar niets aan af. De IT-leverancier werd aansprakelijk geacht voor de schade die het administratiekantoor had geleden door betaling van de bitcoins, de omzetderving en het onderzoek door de ingeschakelde IT-specialist. Wel bleef een deel van de schade voor rekening van het administratiekantoor, omdat dat alleen simpele wachtwoorden wilde gebruiken. De IT-leverancier had hiervoor herhaaldelijk gewaarschuwd. Daarom bleef een derde van de schade voor rekening van het administratiekantoor zelf.

Stof opwaaien

Deze uitspraak deed veel stof opwaaien onder IT-leveranciers. Ze komt er namelijk in feite op neer dat de leverancier ervoor moet zorgen dat afnemers bereid zijn te investeren in beveiligingsmaatregelen. In de uitspraak speelde waarschijnlijk mee dat de IT-leverancier enkel had gesteld dat het administratiekantoor niet mee wilde werken, maar niet dat de beveiliging geen onderdeel was van de opdracht. Verder was er geen schriftelijke overeenkomst waarin doorgaans bepalingen over inspanningsverplichtingen en aansprakelijkheidsbeperkingen zijn opgenomen. Ook dat werkte in dit geval in het nadeel van de IT-leverancier. De afnemer werd aangerekend dat hij de adviezen van de IT-leverancier niet had opgevolgd. Daarom was die aansprakelijk voor een deel van de schade.

Rechters hebben veel vrijheid bij het begroten van de schade en de verdeling ervan over partijen. De balans had in principe dus ook verder richting de afnemer kunnen doorslaan.

Hack tussen SLA's in

Dat laatste blijkt wel uit een uitspraak van het hof Amsterdam, waarin het bepaalde dat twee derde van de schade voor rekening van de afnemer bleef. Het betrof een *service level agreement* (SLA) tussen een IT-leverancier en een klant. De leverancier had de verantwoordelijkheid voor het instandhouden van een adequaat back-upsysteem. Op een gegeven moment wilde de klant overstappen naar een andere leverancier en werd de SLA beëindigd. De overeenkomst met de nieuwe leverancier zou pas zes weken later ingaan. Een maand na het eindigen van de SLA met de oude IT-leverancier werd de klant getroffen door een ransomware-aanval. Deze hack vond dus plaats nadat de SLA met de oude leverancier was geëindigd, maar voordat de SLA met de nieuwe leverancier was ingegaan.

Losgeld in bitcoins

De aanval werd pas opgeheven na het betalen van losgeld van 1371,32 euro in bitcoins. De totale schade van de klant betrof 17.262,27 euro (opzetten noodsysteem, productieverlies, interne uren). De klant stelde de oude IT-leverancier aansprakelijk omdat die het back-upsysteem niet goed had ingesteld. De afnemer kon ten tijde van de aanval daarom niet terugvallen op de laatste, door de IT-leverancier gemaakte back-up. De rechtbank oordeelde dat de oude IT-leverancier niet aansprakelijk kon worden gehouden voor het onderhoud en beheer van het IT-systeem, terwijl de SLA al was geëindigd. In hoger beroep oordeelde het hof dat er op de einddatum van de SLA een recente volledige back-up aanwezig had moeten zijn. Althans, dat deze gereconstrueerd had moeten kunnen worden. De klant had dan nog kunnen terugvallen op een (redelijk) recente back-up.

"Vaak blijkt pas tijdens een hack dat de gemaakte back-ups niet toereikend zijn"

Dagelijkse back-up

Het hof gaf wel aan dat de klant ook schade had geleden als er wel een volledige back-up aanwezig was geweest op de einddatum van de SLA. De hack vond immers vier weken na die datum plaats. Daarom liet het hof twee derde van de door de klant geleden schade voor rekening van de klant zelf komen. Deze uitspraak is gunstiger voor de afnemer dan een eerdere uitspraak van het hof Amsterdam. Toen oordeelde het hof nog dat uit de afspraak voor een dagelijkse back-up niet volgt dat de leverancier dagelijks een back-up van alle volledige bestanden moest maken. De klant moest bepalen van welke bestanden een back-up moest worden gemaakt.

Tips voor de praktijk

Het verschil in de twee uitspraken van het hof Amsterdam wordt mogelijk verklaard doordat de feiten in beide zaken anders waren. De uitspraken illustreren in ieder geval dat heldere afspraken over back-ups essentieel zijn. Denk er daarbij aan om concreet te bepalen hoe vaak en van welke bestanden back-ups moeten worden gemaakt en ook binnen welke termijn deze worden bewaard. Voorkom onduidelijkheid hierover. Kijk ook naar de bepalingen over de aansprakelijkheid in het contract. Vaak wordt aansprakelijkheid voor verlies van data uitgesloten. Als deze bepalingen niet onderhandelbaar blijken, zoals vaak het geval is, onderstreept dat het belang van duidelijke afspraken over de verplichtingen van de IT-leverancier.

Verzwaarde zorgplicht

Beter voorkomen dan genezen uiteraard. Adequate beveiligingsmaatregelen hebben als doel om de hackers buiten de deur te houden. De IT-leverancier heeft op dit gebied een verzwaarde zorgplicht en zal de afnemer indringend en herhaaldelijk moeten waarschuwen als deze zijn adviezen niet opvolgt. Er zal discussie blijven bestaan over de vraag hoeveel hierin kan worden verlangd van de IT-leverancier. Zoals we zagen, vinden rechters dat de afnemer ook een eigen verantwoordelijkheid heeft om dit goed te (laten) regelen.

Conclusie

Cybersecurity is en blijft een onderwerp dat zorgvuldige aandacht vereist. Niet alleen het tegengaan van een ransomware-aanval, maar ook het regelen en inperken van de gevolgen ervan. Van IT-leveranciers wordt verwacht dat zij hun verantwoordelijkheid nemen. Afnemers dienen op hun beurt bereid te zijn hierin te investeren en alert te zijn op goede afspraken hierover. ●