VAST | VERZEKERINGSRECHT AANSPRAKELIJKHEID SCHADE EN TOEZICHT

SPECIAL CYBERRISICO'S: De invloed van de onderliggende overeenkomst op de (bijzondere) zorgplicht van de ICT-beheerder

VAST 2023 / N-021
Rechtbank Overijssel
10 mei 2023, C/08/279512 / HA ZA 22/115

mr. Haarhuis, mr. Thurlings-Rassa, mr. De Moel

BW artikel 6:74 en BW artikel 6:162

Rechtsvraag

Heeft de ICT-beheerder zijn zorgplicht jegens de gemeente geschonden?

In het kort

Op een winterse dinsdag in 2020 wordt de gemeente Hof van Twente geraakt door een ransomware-aanval. De gemeente koos ervoor om niet te betalen, waarna de hackers de systemen hebben vernietigd. De schade liep op tot € 4 miljoen, welke schade de gemeente wil verhalen op haar ICT-beheerder: Switch IT Solutions.

Tussen de gemeente en Switch IT was een overeenkomst van opdracht gesloten via Europese aanbesteding. Daarin was afgesproken dat Switch IT verantwoordelijk was voor 'functionele monitoring' – en dus niet 'security monitoring'. Daarnaast had de gemeente uitdrukkelijk bedongen dat zij een eigen account, dat zij zelf had ingericht en beheerde, behield om externe leveranciers toegang te kunnen geven tot haar netwerk. Aan dit account waren de hoogste beheerrechten gekoppeld, maar er werd geen gebruikgemaakt van de beveiligingstools van Switch IT en evenmin van multifactorauthenticatie. Via dit account zijn de hackers binnengedrongen.

Volgens rechtbank Overijssel had Switch IT – op grond van de overeenkomst – niet de verplichting om beveiligingsincidenten zonder afwijking in het functioneren van het systeem op te merken. Hierdoor kon er ook geen sprake zijn van een onrechtmatige daad. Daarnaast heeft de gemeente zelf, aldus de rechtbank, risico's geschapen – waarvoor zij is gewaarschuwd en die de invulling van de zorgplicht door Switch IT verhinderden. De vorderingen worden afgewezen.

In gelijke zin

Gerechtshof Amsterdam 28 april 2015, ECLI:NL:GHAMS:2015:1635.

In tegengestelde zin

Gerechtshof Amsterdam 16 februari 2021, ECLI:NL:GHAMS:2021:508.

Rechtbank Amsterdam 18 december 2019, ECLI:NL:RBAMS:2019:9635.

Rechtbank Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124.

Tip voor de praktijk

Uit deze uitspraak kunnen twee heldere lessen worden getrokken:

Les 1: leg duidelijk de contractuele afspraken vast. De rechtbank overweegt expliciet dat de verplichtingen zoals contractueel vastgelegd leidend zijn. Het is dus voor alle betrokken partijen van groot belang dat duidelijk is wie waarvoor verantwoordelijk is.

Les 2: als de verantwoordelijkheden verschuiven, bijvoorbeeld door wensen van de klant, is het van belang voor een ICT-beheerder om de klant nadrukkelijk te waarschuwen voor de mogelijke gevolgen daarvan en die waarschuwing ook vast te leggen.

Noot

1. De rechtbank zoomt allereerst in op de overeenkomst tussen partijen, om vast te stellen welke verplichtingen Switch IT jegens de gemeente had. Vooropgesteld wordt dat op grond van het transparantiebeginsel, kort gezegd, alle wensen en eisen van de gemeente bekend moesten zijn. Dit is met name relevant nu de gemeente probeert aanvullende normen van toepassing te verklaren op grond van een verwijzing daarnaar in de toepasselijke GIBIT-voorwaarden. De rechtbank veegt dit echter van tafel met de overweging dat de gemeente in de aanbestedingstukken haar eigen informatiebeveiligingsbeleid als norm heeft gesteld en dat Switch IT daaraan moest voldoen.

2. Ten tweede stelt de rechtbank vast dat partijen functionele monitoring zijn overeengekomen en niet security monitoring. Daarmee mocht van Switch IT wel worden verlangd dat zij signalen opving die van invloed waren op de vereiste beschikbaarheid en vervolgens maatregelen trof. Daarnaast diende Switch IT te zorgen voor een adequate back-up, firewall inrichting en anti-virusmaatregelen. Van Switch IT mocht echter niet worden verlangd dat zij (ook) specifiek op veiligheidsrisico's zou monitoren, zoals bijvoorbeeld door het instellen van een 'alarm' bij een bepaald aantal ongeautoriseerde inlogpogingen.

3. Ten derde is volgens de rechtbank van belang dat de gemeente uitdrukkelijk heeft bedongen dat zij een eigen account behield, dat zij zelf had ingericht en beheerde, om externe leveranciers toegang te kunnen geven tot haar netwerk. Aan dit account waren de hoogste beheerrechten gekoppeld. Op dit beheerdersaccount werd door de gemeente geen gebruik gemaakt van de beveiligingstools of multifactorauthenticatie, en toevalligerwijs was dit account de ingang voor de hackers.

4. Ten vierde haalt de rechtbank expliciet uit het onderzoek van Cyber Specialist NFIR aan dat door de gemeente zelf een regel in de firewall is aangepast waardoor iedereen op het internet verbinding kon zoeken met de FTP-server van de gemeente. Volgens de rechtbank is daarna door een medewerker van de gemeente een zwak wachtwoord ('Welkom2020') ingesteld voor het beheerdersaccount. Het opstellen van het wachtwoordbeleid in verband met de toegang tot de accounts was eveneens de verantwoordelijkheid van de gemeente. Overigens volgt uit het rapport van onderzoeksjournalist Brenno de Winter dat de wachtwoordverandering *vooraf* ging aan de aanpassing van de firewall. De rechtbank signaleert dat Switch IT niet op de hoogte was gesteld van deze aanpassingen.

5. Tot slot benoemt de rechtbank meerdere keren dat Switch IT Hof van Twente heeft gewezen op de risico's die gepaard gingen met het eigen beheerdersaccount. Ook de accountant van de gemeente heeft diverse keren gewaarschuwd voor de risico's op het gebied van informatiebeveiliging en cyberaanvallen.

6. In het licht van het voorgaande overweegt de rechtbank als volgt. Door de gemeente is onvoldoende onderbouwd dat de aanval (ook) een impact heeft gehad op het functioneren van het netwerk. Evenmin is onderbouwd dat het aanpassen van de firewall een signaal had moeten zijn voor Switch IT. Op grond van de overeenkomst had Switch IT volgens de rechtbank niet de verplichting de monitoring zo in te richten dat beveiligingsincidenten, ook zonder dat die tot afwijkingen in het functioneren leidde, gesignaleerd werden. Bovendien wijst de rechtbank erop dat het wachtwoordbeleid de verantwoordelijkheid van de gemeente was, en het voor de hackers gemakkelijk te raden wachtwoord 'Welkom 2020' daaraan voldeed. De rechtbank concludeert dat Switch IT niet tekort is geschoten in de nakoming van de verplichting tot proactieve monitoring.

7. Naast dit voornaamste onderdeel van de overeenkomst heeft de gemeente Switch IT ook zorgplichtschendingen door onvoldoende borging van de back-up, anti-virusmaatregelen en inrichting van de firewall verweten. De rechtbank veegt ook deze gestelde schendingen van tafel. Ten aanzien van de back-up had Switch IT een voorstel gedaan tot back-up hardening (het isoleren van de back-up), was de gemeente gewaarschuwd voor de risico's en leek deze verplichting eerder op de vorige ICT-beheerder te rusten. Ten aanzien van de anti-virusmaatregelen was (mede doordat bewijs verloren was gegaan als gevolg van de hack) onvoldoende aangetoond dat dit niet goed geborgd was. Tot slot wordt ten aanzien van de firewallinrichting herhaald dat de gemeente er zelf voor heeft gekozen om voor de firewallinrichting geen security monitoring overeen te komen en die ene regel aan te passen.

8. Kortom, ook deze verwijten leiden niet tot een zorgplichtschending. De rechtbank stelt zich vervolgens hardop de vraag of, naast de verplichtingen in het contract, er nog andere eisen gesteld kunnen worden aan de zorgplicht ex artikel 6:162 BW. Eerder had de rechtbank al overwogen dat als er een overeenkomst met een ICT-beheerder is gesloten voor specifieke diensten, het juist van de inhoud van die overeenkomst afhangt wat er van de ICT-beheerder mag worden verwacht. Daarmee werd eigenlijk al een streep gezet door het subsidiaire beroep op onrechtmatige daad. Ter aanvulling daarop overweegt de rechtbank nog dat de zorgplicht van een ICT-beheerder niet zover gaat dat, als functionele monitoring overeengekomen is, security monitoring daar (kennelijk gratis) onderdeel van uitmaakt. Dit onder verwijzing naar het eigen handelen van de gemeente en de door Switch IT gegeven waarschuwingen. De vorderingen van de gemeente worden afgewezen en de gemeente wordt veroordeeld in de proceskosten.

9. Deze uitspraak is opvallend omdat de zorgplicht van de ICT-beheerder meer in proportie lijkt te worden gebracht met de expliciete wensen van de klant. In eerdere uitspraken werd veelal uitgegaan van een bijzondere zorgplicht van de ICT-beheerder. Dit nu de ICT-dienstverlening meestal wordt uitbesteed door een gebrek aan kennis daarover, terwijl de ingeschakelde ICT-beheerder bij uitstek de kennis en expertise in huis heeft.

10. Zo oordeelde de rechtbank Amsterdam in 2019 (ECLI:NL:RBAMS:2019:9635) dat van de ICT-beheerder verwacht mocht worden dat hij een CRM-systeem opleverde dat voldeed aan de verwachtingen van een gemiddelde klant – ook als dat niet met zoveel woorden in de overeenkomst was opgenomen. Daarnaast mocht de klant verwachten dat normen die niet uitdrukkelijk waren overeengekomen, maar wel in de branche gebruikelijk waren, in acht werden genomen. Opmerking verdient hier dat de overeenkomst in die zaak een stuk minder uitgebreid was (lees: een PowerPoint presentatie).

11. Daarvoor, in 2018, heeft de rechtbank Amsterdam uitspraak gedaan (ECLI:NL:RBAMS:2018:10124) in een zaak waarin de ICT-beheerder zich onder andere verdedigde met de stelling dat de klant bepaalde beveiligingsmaatregelen van de hand had gewezen in verband met de daarmee gepaard gaande kosten en het 'gedoe'. De rechtbank oordeelde daarover dat het op de weg van de ICT-beheerder had gelegen om op zijn minst 'indringend en herhaaldelijk' te waarschuwen voor de daarmee gepaard gaande risico's. Ondanks dat de klant zelf ook kennis van zaken had het gebied op van IT, diende de ICT-beheerder – gelet op de afspraak dat een totaalpakket werd geleverd en zijn professionele deskundigheid – meer te doen dan enkel waarschuwen en vervolgens berusten in de keuzes van de klant.

12. Ook in een overgangsperiode, waarbij de opvolgende ICT-beheerder al wijzigingen aan het doorvoeren was in de digitale infrastructuur maar het contract van de 'oude' ICT-beheerder officieel nog gold, kon de 'oude' ICT-beheerder volledig aan de verplichtingen in de overeenkomst worden gehouden, aldus het hof Amsterdam in 2021 (ECLI:NL:GHAMS:2021:508). Daarbij overwoog het hof dat het op de weg van de ICT-beheerder lag om aan te tonen dat bepaalde verantwoordelijkheden waren overgegaan naar de opvolgende ICT-beheerder.

13. Interessant in deze uitspraak van het hof is dat de ICT-beheerder volgens het hof dient op te draaien voor het betaalde losgeld, nu de klant volgens het hof door het ontbreken van een recente back-up ertoe werd gedwongen om het losgeld te betalen. Twee alinea's verder haalt het hof aan dat de politie de klant met klem had aangeraden om helemaal geen losgeld te betalen, waardoor een 'last minute' betaling ook niet aan de klant wordt toegerekend. Over het wel of niet betalen van losgeld bij een ransomware-aanval wordt in de praktijk hevig gediscussieerd: dit vraagstuk wordt veelal gezien als een ethisch dilemma. De overweging van het hof dat, bij het ontbreken van een recente back-up, een klant gedwongen wordt om losgeld te betalen, biedt steun aan de voorstanders van het betalen van losgeld om hogere schade te voorkomen. Ter illustratie: Hof van Twente had voor een losgeldbedrag van € 750.000 een schade van € 4.000.000 kunnen afkopen. Het voornaamste tegenargument is dat door betaling het businessmodel van de hackers in stand wordt gehouden. Deze instandhouding wordt naar mijn mening versterkt als een klant een dergelijke schadepost in voorkomende gevallen op de ICT-beheerder kan verhalen.

14. Als laatste dient nog vermeld te worden dat in de uitspraak van het hof een schuldverdeling van twee derde in het nadeel van de klant werd gehanteerd. Daarmee komt de ontstane onduidelijkheid tijdens de overgangsperiode (met tussen de contracten een 'gat' van anderhalve maand waarin de hack plaatsvond) toch grotendeels voor rekening van de klant.

15. Kortom, de stand van zaken tot aan deze uitspraak was dat het contract een eerste aanknopingspunt was voor de omvang van de zorgplicht van de ICT-beheerder, maar dat daar – op

basis van de bijzondere zorgplicht – extra verplichtingen bij konden komen. In deze uitspraak wordt dit uitgangspunt in zoverre genuanceerd dat het contract leidend is en er daarnaast geen ruimte wordt gezien voor aanvullende verplichtingen die niet zijn vastgelegd, zeker niet als er nadrukkelijk voor de risico's is gewaarschuwd. Daarmee zouden ICT-beheerders beter weten waar ze aan toe zijn, ervan uitgaande dat de afspraken duidelijk zijn vastgelegd in de overeenkomst. Of deze nuancering alleen voor een overeenkomst uit aanbesteding stand gaat houden of breder van toepassing wordt, zal moeten worden afgewacht.

Keywords

Aansprakelijkheidsrecht
Beroepsaansprakelijkheid
Cyberaanval
Ransomware-aanval
Verbintenissenrecht
Zorgvuldigheidsnorm ICT-beheerder

Vindplaatsen

ECLI:NL:RBOVE:2023:1731

Auteur(s)

Eline van Hal

Advocaat bij V&A Advocaten

LinkedIn