Raadsbrief

Onderwerp	Arrest gerechtshof n.a.v. hoger beroep hack
Zaaknummer	886618
Datum	6 maart 2025
Portefeuillehouder	drs. H.A.M. Nauta-van Moorsel MPM
Team	Concernstaf

Doel
Ter informatie.

Aanleiding
Op 25 februari 2025 heeft het gerechtshof Arnhem-Leeuwarden uitspraak gedaan in het hoger beroep dat de gemeente instelde tegen de vonnissen van de rechtbank Overijssel in de dagvaardingsprocedure tegen Switch IT Solutions/Dustin (hierna Switch). De raad ontving deze uitspraak op dezelfde datum ter informatie van ons.

Zoals bekend eiste de gemeente Hof van Twente in een civiele procedure die in 2021 is gestart een schadevergoeding van deze ICT-leverancier. Switch was ten tijde van de cyber-aanval in december 2020 voor de gemeente werkzaam op het gebied van systeembeheer en overige ICT-dienstverlening. De gemeente stelde zich op het standpunt dat we weliswaar zelf mede schuldig waren aan het kunnen ontstaan van de hack, maar dat dit ook gold voor Switch, die haar contractuele en wettelijke verplichtingen niet goed was nagekomen. In juridische termen heeft zij tegenover de gemeente wanprestatie gepleegd, haar zorgplicht als professioneel ICT-bedrijf geschonden en onrechtmatig gehandeld.

Het gerechtshof komt net als de rechtbank tot de conclusie dat de vorderingen van de gemeente naar haar oordeel niet toewijsbaar zijn en heeft de vonnissen van de rechtbank daarom bekrachtigd. Dit betekent dat de gemeente in het ongelijk is gesteld, de gemeente geen schadevergoeding ontvangt en veroordeeld is tot het betalen van de proceskosten.

Wij zijn met oprechte intenties en op goede en weloverwogen gronden in hoger beroep gegaan bij het gerechtshof. Voor ons stond de principiële vraag centraal hoe de verant-woordelijkheden tussen de gemeente als opdrachtgever en haar ICT-dienstverlener als opdrachtnemer zich tot elkaar verhouden.

Wij waren ervan overtuigd dat zowel onze ICT-dienstverlener als wij als gemeente in redelijkheid een gedeelde verantwoordelijkheid droegen voor het ontstaan van de hack en de daaruit voortvloeiende schade. Maar we kunnen nu niet anders constateren dan dat ons juridisch betoog geen steun vindt bij de rechter.

In deze raadsbrief geven wij een terugblik op de vraag waarom de gemeente in hoger beroep is gegaan en welke afweging destijds is gemaakt. Daarna presenteren we een samenvatting van de strekking van het arrest. Vervolgens geven wij aan wat dit arrest voor de gemeente betekent en welke conclusies wij hieruit trekken. We gaan in op de vraag of er aanleiding bestaat voor het instellen van cassatie bij de Hoge Raad en verwoorden tot slot hoe wij nu verder willen gaan.

Inhoudelijke boodschap

Waarom heeft de gemeente in 2023 besloten tot het instellen van hoger beroep?
Op 10 mei 2023 heeft de rechtbank Overijssel uitspraak gedaan in de door de gemeente aangespannen dagvaardingsprocedure tegen Switch. In dat vonnis wees de rechtbank de vorderingen van de gemeente af. Vanaf de start van de juridische procedure stond voor ons college de principiële vraag centraal hoe de verantwoordelijkheden tussen de gemeente als opdrachtgever en een ICT-dienstverlener als opdrachtnemer zich tot elkaar verhouden. Daarom was het wenselijk dat ook een hogere rechter zich over de kwestie zou buigen. Dit kwam mede voort uit onze overtuiging, na overleg met juristen, dat sommige juridische aspecten bij de rechtbank onderbelicht waren gebleven.

Vanwege deze overwegingen doorliep het college in de zomer van 2023 een besluit-vormingstraject over de vraag of de gemeente in hoger beroep zou gaan. Hiervoor is een objectieve belangenafweging gemaakt en zijn diverse opvattingen verzameld, die een basis boden voor een gedegen afweging en een gefundeerde keuze.

Welke belangen zijn afgewogen voorafgaand aan het hoger beroep?

Brainstorm en adviezen ingewonnen
In de periode mei-juli 2023 hebben wij actief met diverse personen van binnen en buiten de organisatie gesproken over de vraag of het wenselijk en zinvol zou zijn om in hoger beroep te gaan. Tijdens een brainstorm op 6 juni 2023 in het gemeentehuis werden meningen gepeild van de directeur van Informatiebeveiligingsdienst (IBD) van de VNG, de directeur van onderzoeksbureau NFIR, een publicist/ICT-deskundige, onze advocaat en een second-opinion advocaat. Ook vond op 20 juni 2023 een overleg plaats met een delegatie van de VNG en IBD. Dit vanwege de mogelijke impact van nieuwe jurisprudentie over de wettelijke en contractuele zorgplicht van ICT-leveranciers tegenover gemeentelijke opdrachtgevers.

Juridisch advies ingewonnen
Er is een juridisch advies gevraagd en ontvangen van onze advocaat mr. dr. A.W. Duthler van Advocatenkantoor First Lawyers uit Den Haag. Daarin lichtte zij toe welke juridische argumentatie gebruikt kon worden in het hoger beroep. De perceptie dat de rechtbank op enkele cruciale punten een onjuiste of onvolledige uitleg heeft gegeven aan geldende regelgeving maakte dat de advocaat het instellen van hoger beroep een reële stap vond. Zij concludeerde dat er duidelijke juridische handvatten waren om in hoger beroep te gaan en de rechtsvinding een vervolg te geven.

Afwegingskader
Tot slot hebben wij op basis van de verzamelde inzichten een afwegingskader ontwikkeld. Hierin is een algemene analyse gemaakt van de belangen die in de afweging een rol konden spelen. Dit afwegingskader, dat wij op 11 juli 2023 met de gemeenteraad hebben besproken, leidde tot de conclusie dat er objectief bezien voldoende aanleiding bestond om in hoger beroep te gaan. Deze belangen waren de volgende:

- **Lokaal juridisch belang:** De leverancier moest aangesproken kunnen worden op nalatig en onrechtmatig handelen. Dit neemt niet weg dat wij altijd transparant zijn geweest over het feit dat de gemeente mede schuld draagt voor onder haar verantwoordelijkheid gemaakte fouten.
- **Landelijk juridisch belang**: Naar verwachting zou het hoger beroep kunnen leiden tot een algemene rechtsregel die voor andere gemeenten van belang kan zijn.
- **Bestuurlijk belang**: Een arrest zou kunnen leiden tot een afronding van het dossier over de cyberaanval.
- **Financieel belang:** Door het honoreren van de claim zou de gemeente een deel van de geleden schade vergoed kunnen krijgen. De schade die direct en indirect is veroorzaakt als gevolg van de hack in de crisisfase en de noodzakelijke wederopbouw van de ICT-infrastructuur is medio 2021 vastgesteld op ongeveer € 4,2 miljoen.

- **Politiek belang**: Na de eerste drie onderzoeksrapporten vonden medio 2021 politieke debatten plaats over de informatieveiligheid en het contractmanagement. Het college vertaalde de aanbevelingen naar concrete verbeteracties in het Verbeterplan hack. Hierover is nadien meerdere keren gerapporteerd richting de raad en de raadscommissie Informatieveiligheid.
- **Imagobelang**: Een uitspraak in hoger beroep kon van invloed zijn op de beeldvorming over de hack, wanneer het hof ontvankelijk zou zijn voor onze juridische argumentatie en onderbouwing.
- **Ethisch belang**: De keuze om te gaan dagvaarden zou mede ingegeven kunnen worden door het ethische bewustzijn dat leveranciers van ICT-diensten aangesproken moeten kunnen worden op fouten.
- **Werkgeversbelang:** De cyberaanval heeft onze organisatie geraakt. Medewerkers die betrokken waren bij het beheer van de ICT-infrastructuur, collegeleden, maar ook iedereen die na de hack een enorme inspanning heeft moeten leveren om de dienstverlening weer op peil te brengen en systemen en dataverzamelingen weer “up and running” te krijgen.

Wat waren de juridische argumenten van de gemeente om in hoger beroep te gaan?
In de kern hielden de verwijten die de gemeente aan Switch maakte het volgende in:

Ten eerste had Switch de ongebruikelijke hoeveelheid inlogpogingen in het jaar voorafgaand aan de hack van 1 december 2020 kunnen voorkomen als zij de firewall adequaat had ingericht en beheerd. In technische bewoordingen: de openstaande poort (RDP-faciliteit) had automatisch moeten worden uitgezet na verloop van een korte tijd nadat deze na gebruik (voor technisch onderhoud) onbedoeld open was blijven staan.

Ten tweede had Switch de ongebruikelijke hoeveelheid inlogpogingen (honderdduizenden) moeten signaleren, zodat de cyberaanvallers gestopt hadden kunnen worden met hun zogeheten “brute force aanval” die aan de hack vooraf ging. De hack zou hierdoor niet hebben plaatsgevonden.

Ten derde had Switch de back-up voorziening veilig moeten inrichten volgens het zogeheten 3-2-1-principe. Daarbij had een (derde) kopie van alle back-up data elders (‘off-site’) veilig moeten worden bewaard, zodat deze buiten bereik van onbevoegden (hackers) zou zijn gebleven en de schade was voorkomen of in ieder geval beperkt zou zijn gebleven.

Welke argumenten heeft het gerechtshof gebruikt om tot haar oordeel te komen?
Het Hof gaat in het arrest in op de inhoud van de overeenkomst en de verplichtingen die hieruit volgen, de verwijten die de gemeente Switch maakt op basis daarvan, de schending van de zorgplicht en de onrechtmatige daad. Het arrest wordt afgesloten met een beslissing.

Het Hof stelt dat Switch op basis van de **inhoud van de overeenkomst** als taak had het systeembeheer en aanverwante ICT-beheerdienstverlening van de gemeente te verzorgen. Switch was verantwoordelijk voor het configuratiebeheer van de servers, opslag en netwerkvoorzieningen en de gemeente was verantwoordelijk voor de overige apparatuur. Het Hof oordeelt op basis van de inhoud van de overeenkomst als volgt:

Er was volgens het Hof sprake van duaal beheer omdat de gemeente een eigen account (met de hoogste beheerrechten) wilde behouden. Aangezien sprake is van duaal beheer had de gemeente wijzigingen, die via het beheeraccount werden doorgevoerd (zoals het wijzigen van de regel in de firewall en het wijzigen van het wachtwoord) door moeten geven aan Switch. Switch volgde de ‘best practices’, niet zijnde BIG en BIO, en productontwikkeling en vervulde daarvoor een voortdurende en proactieve adviesrol in de richting van de gemeente.

Switch beheerde objecten op beschikbaarheid, capaciteit en performance, niet op securitymonitoring. De beschikbaarheid van het netwerk betrof geen veiligheidsaspect.
Er was volgens het Hof sprake van een inspanningsverplichting voor Switch. In de opdracht stond immers niet een verplichting om een bepaald resultaat tot stand te brengen.
Ten aanzien van de **verwijten van de gemeente** jegens Switch, oordeelt het Hof als volgt:

Het beheer van de firewall was een activiteit die voortdurende zorg vroeg. Hieruit volgt niet dat Switch het logboek van de firewall moest controleren om verdachte activiteiten op te sporen en waar nodig beschermingsmaatregelen te nemen of voor te stellen.
Niet gebleken is dat de vele inlogpogingen of brute force aanvallen van (werkelijke) invloed zijn geweest op de performance waarvoor Switch wel de verantwoordelijkheid droeg.
De gemeente heeft volgens het Hof niets ingebracht tegen het verweer van Switch dat sprake was van een 3-2-1 off-site back-up. Bovendien lag de oorzaak van de aanval niet in een onjuiste inrichting van de back-upvoorziening, maar in het feit dat de hackers toegang hebben verkregen via het hoogste domeinadministrator account van de gemeente en daardoor ook toegang kregen tot de back-ups. De conclusie van het Hof is dat van een tekortkoming op de door de gemeente genoemde punten niet is gebleken. De vorderingen zijn op deze grondslag dan ook volgens het Hof niet toewijsbaar.

Vervolgens komt het Hof tot het oordeel dat geen sprake is van **schending van de zorgplicht** door Switch. Hiertoe overweegt zij het volgende:
Switch heeft voldoende toegelicht dat zij met de bestaande back-up oplossing aan de door de gemeente gestelde eisen voldeed. Switch hoefde zich niet bezig te houden met netwerk-segmentatie omdat haar voorganger dit zou uitvoeren en dit dus buiten de scope van de opdracht viel. Switch mocht verwachten dat de gemeente voldoende kennis in huis had om verantwoord om te gaan met het behoud van beheerrechten. En Switch heeft de gemeente afdoende geïnformeerd over het instellen van multifactor authenticatie (MFA) op de door haar beheerde accounts, zodat daarop volgens het Hof geen beperkingen van het aantal foutieve inlogpogingen hoefden te worden ingesteld.

Er is volgens het Hof geen sprake van een **onrechtmatige daad.** De door de gemeente gestelde tekortkomingen zijn immers niet komen vast te staan. Als **beslissing** bekrachtigt het Hof de vonnissen van de rechtbank en wijst zij af wat verder gevorderd is.

Welke conclusies trekken wij uit het arrest van het Hof?

Duidelijkheid over (mede)verantwoordelijkheid
Hoewel de uitkomst niet was zoals gehoopt en Switch volgens het Hof geen enkele mede-verantwoordelijkheid draagt voor de schade die door de hack is ontstaan, geeft het arrest wel de gewenste duidelijkheid. Het bevestigt dat een gemeente als opdrachtgever van een leverancier van ICT-systeembeheersdiensten altijd volledig verantwoordelijk blijft voor de informatieveiligheid in brede zin (ook als je onderdelen zoals de back up en firewall uitbesteedt) en daar zelf de nodige inhoudelijke expertise voor moet organiseren. Maar het arrest biedt ook duidelijkheid over het principiële inzicht dat op een leverancier van ICT-diensten uitsluitend een inspanningsverplichting rust en géén resultaatverplichting; zelfs niet wanneer er voor specifieke verplichtingen garanties zijn afgesproken.

Contractuele verplichtingen vastleggen
Een andere les is dat contractuele verplichtingen altijd expliciet moeten worden vastgelegd op basis van aanbestedingsdocumenten, contracten en aanvullende schriftelijke afspraken. Verwijzingen naar toepasselijke algemene GIBIT-voorwaarden (deze zijn door de VNG ontwikkeld en worden door gemeenten gezien als best-practices) en wettelijke normen waar gemeenten aan gebonden zijn, leiden er niet toe dat ook een leverancier hier rechtstreeks aan gebonden is. Bovendien zijn vormen van samenwerking, waarbij opdrachtgever en opdrachtnemer beiden naast elkaar (delen) van ICT-werkzaamheden blijven verrichten niet gewenst. Het gerechtshof stelt dat Hof van Twente een vorm van duaal beheer had laten ontstaan, waar zij zelf volledig voor verantwoordelijk te houden is.

Inhoudelijke opdrachtgeversrol vervullen
Aan een opdrachtgever worden eisen gesteld zowel bij de opstelling van een contract als bij de naleving ervan. Het arrest bevestigt duidelijk dat de gemeente gedurende de looptijd van een ICT-dienstverleningscontract actief een professionele opdrachtgeversrol moet vervullen. De eerdergenoemde onderzoeksrapporten uit 2021 wezen hier ook op. De professionalisering van het opdrachtgeverschap vormde daarom één van de actiepunten uit het Verbeterprogramma hack. Dat programma hebben wij tot en met 2023 gebruikt, onder meer om de Autoriteit persoonsgegevens (AP) te informeren over de wederopbouw na de hack.

Concrete resultaten van het Verbeterprogramma hack in onze organisatie zijn zowel de inrichting van een cluster Inkoop in het team Beleid & Advies als de vorming van het Regiebureau Informatisering & Automatisering. Beide betreft het ontwikkelingen waar de raad in de afgelopen jaren groen licht voor heeft gegeven.

Landelijk samenwerken en aandacht vragen
In de afgelopen jaren is er vanuit Hof van Twente een intensieve samenwerking ontstaan met de informatiebeveiligingsdienst (IBD) van de VNG. Deze organisatie heeft haar dienstverlening richting gemeenten rondom crisisbeheersing, mede in reactie op onze hack, sterk ontwikkeld. Vanuit Hof van Twente is actief meegedacht in kennisontwikkeling en -deling, bijvoorbeeld in de vorm van ambtelijke instructies, bestuurlijke handreikingen ed. Het hoger beroep werd dan ook met grote belangstelling vanuit bestuurlijk Nederland gevolgd. Steeds meer gemeenten achten zich door de complexiteit van ICT, data- en systeembeheer en het groeiende normenstelsel van informatieveiligheid niet meer in staat om zelf de taakuitvoering in eigen regie te organiseren. Tegelijk toont de casus Hof van Twente dat uitbesteding van dienstverlening gemeenten niet hun (grote) verantwoordelijkheid ontneemt.

Externe toetsingen laten uitvoeren
Hof van Twente heeft in 2023-2024 een externe audit laten uitvoeren naar onze ICT-infrastructuur en informatieveiligheid door bureau JoanKnecht uit Eindhoven. De raad is hier via de raadscommissie Informatieveiligheid enkele malen over geïnformeerd. Het arrest van het Hof onderstreept het belang van regelmatige externe toetsingen. Niet alleen de gemeente, maar ook de ingehuurde externe ICT-leveranciers worden hierbij nauwgezet onderzocht om te beoordelen of zij voldoen aan wettelijke standaarden en normen. In ons jaarprogramma informatieveiligheid & privacy zullen wij periodiek externe onderzoeken zoals deze audit blijven opnemen.

Verwerking financiële gevolgen arrest
Al in 2021 bleek uit onderzoek van NFIR dat we er (gelukkig) vanuit mochten gaan dat geen privacygevoelige data voortkomende uit de hack in handen van de hackers zijn gekomen, en dus ook niet op straat zijn beland. Tegelijk realiseren wij ons dat nu definitief is komen vast te staan dat de gemeente zelf de kosten van de hack dient te dragen. In dit verband wijzen wij er opnieuw op, dat de gemeente deze kosten al in de begrotingen c.q. jaarrekeningen van afgelopen jaren heeft verwerkt. Dit geldt ook voor de juridische kosten die met de rechtsgang gemoeid waren. Dat betekent dat op dit moment uitsluitend de proceskosten tot een nieuwe autonome ontwikkeling leiden. Deze zullen wij in de eerste Bestuursrapportage 2025 opnemen.

Het vervolg
Met het uitbrengen van het arrest door het Hof ontstaat de wettelijke mogelijkheid om beroep in cassatie in te stellen bij de Hoge Raad. Cassatie vormt een ultieme juridische stap in een civiele dagvaardingsprocedure. De gemeente heeft een dergelijke stap jaren geleden (met succes) gezet in een andere zaak, namelijk de zogeheten Landgoed Hof van Twente casus. Om cassatie te kunnen instellen dient een expliciete interpretatie van juridische regelgeving in het geding te zijn. De constellatie van feiten komt daarbij niet meer aan bod.

Wij zijn, mede na overleg met onze advocaat en interne juridische adviseurs, tot het inzicht gekomen dat het niet waarschijnlijk is dat in de huidige casus er een reële verwachting bestaat dat een beroep in cassatie kans van slagen zal hebben, ook al zouden hier mogelijk aanknopingspunten voor kunnen bestaan. We zien daarom af van een dergelijk vervolg.

Wel willen we op basis van deze raadsbrief graag in gesprek met de raadscommissie Informatieveiligheid. Deze commissie is naar aanleiding van de hack ingesteld en is in samenwerking met de CISO al geruime tijd betrokken om de adviezen uit de verschillende rapporten over de hack te bespreken en te volgen hoe deze geïmplementeerd worden in de organisatie. Dit gesprek kan gaan over onze analyse en aanpak, maar ook over de mogelijke en wenselijke keuzes die we kunnen/moeten maken waar het gaat om de duurzaamheid van onze ICT op de langere termijn. Wij kunnen ons voorstellen dat de gemeenteraad de raadsbrief vervolgens wil agenderen voor een raadsvergadering.

Conclusie

Met deze raadsbrief hebben wij het proces van de afgelopen jaren rondom de zogenaamde ‘juridische procedure hack’ uiteengezet. Wij hebben geprobeerd de ontwikkelingen in perspectief te plaatsen. Wij benadrukken opnieuw dat wij als college met oprechte intenties en weloverwogen gronden in hoger beroep zijn gegaan bij het gerechtshof. Voor ons stond de principiële vraag centraal hoe de verantwoordelijkheden tussen de gemeente als opdrachtgever en haar ICT-dienstverlener als opdrachtnemer zich tot elkaar verhouden.

Onze overtuiging was dat in redelijkheid sprake was van een gedeelde verantwoordelijkheid bij onze ICT-dienstverlener en ons als gemeente voor het ontstaan van de hack en de hieruit voortkomende schade. Helaas vond ons juridische betoog geen steun bij de rechter, niet in eerste aanleg en niet in hoger beroep. Wij zullen echter géén beroep in cassatie instellen.

Burgemeester en wethouders van Hof van Twente,

de secretaris,	de burgemeester,
drs. D. Lacroix	drs. H.A.M. Nauta-van Moorsel MPM