

## Nieuws



## Ict-bedrijf aansprakelijk voor schade van ransomware-aanval bij klant

woensdag 11 september 2024, 13:56 door [Redactie](#), 14 [reacties](#)

Een ict-dienstverlener uit Coevorden is aansprakelijk voor de schade die een ransomware-aanval bij een klant veroorzaakte, zo heeft de rechtbank **Noord-Nederland geoordeeld**. Het ict-bedrijf verzorgde het netwerkbeheer voor de klant, die in oktober 2019 door een ransomware-aanval werd getroffen. Hierbij werden bestanden op systemen alsmede de back-ups versleuteld. De klant heeft de aanvallers geen losgeld betaald.


Volgens de klant was de ransomware-aanval mogelijk door zes risicofactoren: RDP-poorten stonden open; er werd geen ip-adres whitelisting toegepast; de wachtwoorden die het ict-bedrijf gebruikte voor het uitvoeren van het beheer voor de servers waren één en dezelfde en bovendien gemakkelijk te achterhalen; er was geen netwerksegmentatie toegepast; updates van servers waren niet doorgevoerd; en een server die al jaren buiten service was en niet meer werd gebruikt, was niet uitgezet, maar hing nog steeds onbeveiligd aan het internet.

De klant liet onderzoek naar de ransomware-aanval uitvoeren, maar er kon niet worden achterhaald hoe de aanvallers toegang tot het netwerk hadden gekregen. Hoe de aanvallers het netwerk konden binnendringen kan volgens de rechter in het midden blijven. Van belang is dat schade is ontstaan doordat bij de aanval niet alleen de werkbestanden maar ook de back-ups versleuteld werden. "Netwerksegmentatie, een beter wachtwoordbeleid en een deugdelijk afgescheiden back-upvoorziening hadden dat kunnen voorkomen", aldus de rechter.

De rechtbank is van oordeel dat het ict-bedrijf toerekenbaar tekort is geschoten in haar verplichtingen uit de netwerkbeheerovereenkomst door de klant niet in duidelijke bewoordingen te wijzen op het ontbreken van netwerksegmentatie, de kwetsbaarheid van de back-upvoorziening en het gebrekkige wachtwoordbeleid, en de daarmee gepaard gaande beveiligingsrisico's. Het ict-bedrijf is dan ook aansprakelijk voor de schade die de klant als gevolg van deze tekortkoming heeft geleden, aldus de rechter.

De klant eiste dat het ict-bedrijf vergoedingen van bij elkaar één miljoen euro zou betalen. Het ict-bedrijf stelde dat de aansprakelijkheid is beperkt tot vijftigduizend euro. De rechter gaat niet mee in de eis van de klant. Zo komen de kosten van forensisch onderzoek en mitigatie niet voor schadevergoeding in aanmerking en zijn de door de klant genoemde schadebedragen niet zodanig disproportioneel dat hierdoor een beroep op de aansprakelijkheidsbeperking onaanvaardbaar zou zijn. De rechter wijst de vordering van de klant dan ook toe tot een bedrag van vijftigduizend euro.

 [Douane trekt aanbesteding voor aanschaf mobiele containerscanners in](#)

 [Szabó: rijksoverheid heeft geen geschikt alternatief voor Cisco Webex](#)

## Reacties (14)

11-09-2024, 14:14 door Anoniem

[Reageer met quote](#) 

Kortom: knoeien kost max. 50k. Dan kan de rekensom gemaakt worden.

11-09-2024, 14:55 door Anoniem

[Reageer met quote](#) 

Voor een klant die al die feiten kan opdreunen zoals:

*'RDP-poorten stonden open; er werd geen ip-adres whitelisting toegepast; de wachtwoorden die het ict-bedrijf gebruikte voor het uitvoeren van het beheer voor de servers waren één en dezelfde en bovendien gemakkelijk te achterhalen; er was geen netwerksegmentatie toegepast; updates van servers waren niet doorgevoerd; en een server die al jaren buiten service was en niet meer werd gebruikt, was niet uitgezet, maar hing nog steeds onbeveiligd aan het internet.'*

Allemaal uiteraard na een extern onderzoek, moet zelf ook maar eens in de spiegel kijken, want een externe audit op zijn tijd is zeker aan te bevelen.

11-09-2024, 14:57 door Anoniem

[Reageer met quote](#) 

*Door Anoniem:* Kortom: knoeien kost max. 50k. Dan kan de rekensom gemaakt worden.

Dat hangt af van de dienstverleningsovereenkomst die je afsluit. Als klant kun je daarin prima hogere bedragen voor schadevergoeding laten opnemen. Als je leverancier daarmee akkoord gaat dan ben je voor een hoger bedrag gedekt.

11-09-2024, 16:31 door Anoniem

[Reageer met quote](#) 

*Door Anoniem:*

*Door Anoniem:* Kortom: knoeien kost max. 50k. Dan kan de rekensom gemaakt worden.

Dat hangt af van de dienstverleningsovereenkomst die je afsluit. Als klant kun je daarin prima hogere bedragen voor schadevergoeding laten opnemen. Als je leverancier daarmee akkoord gaat dan ben je voor een hoger bedrag gedekt.

Natuurlijk alleen nadat je de leverancier ook nog aansprakelijk gesteld hebt , en die dat erkend heeft - of de rechter dat besloten heeft .  
En de geclaimde schade ook onderbouwd is .

Je wordt er zelden of nooit 'beter' van als je schadeclaims (of verzekeringsuitkeringen - zelfde) toegewezen krijgt.

Natuurlijk is het beter dan niks , maar praktisch altijd kost je het ergens tijd/moeite/ergernis om weer 'terug te komen waar je was' .

11-09-2024, 19:46 door Anoniem

[Reageer met quote](#) 

Goh, extern inhuren is toch altijd beter . Gnif gnif. Die kleine mkb ict bedrijfjes hebben de kennis gewoon niet om dit soort zaken gewoon goed op orde te hebben. Als je met een paar man een 'ict bedrijf' runt dan is er vaak gewoon niet kennis of mankracht genoeg voor dit soort zaken OF het moet allemaal zo goedkoop mogelijk ( van de klant en voor de dienstverlener zelf ).

11-09-2024, 19:48 door Anoniem

[Reageer met quote](#) 

Zoeken



## Vacature



Rijksoverheid

### Information Security Officer (ISO)

#### Dienst Justitiële Inrichtingen

Ben jij een tech-liefhebber met een passie voor informatiebeveiliging? Wil je jouw expertise inzetten om de veiligheid te waarborgen binnen een dynamische omgeving? Dan is de rol van Informatiebeveiligingsfunctionaris bij Justitieel Complex Zaanstad wellicht jouw volgende avontuur! In deze rol ben jij de sleutel tot het creëren en handhaven van een veilige werkomgeving, waarbij onze organisatie optimaal blijft draaien.

[Lees meer](#) 

## Privacyvriendelijke leeftijdsverificatie:

- ☐ Kansloos
- ☐ Het proberen waard
- ☐ ' OR '1'=1

Aantal stemmen: **945** [17 reacties](#)


## Vacature



Gemeente Utrecht

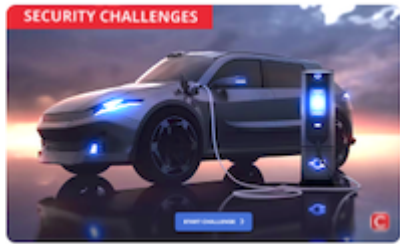
### Chief Information Security Officer

Utrecht heeft jou nodig! Als Chief Information Security Officer speel jij een cruciale rol in de bescherming van de digitale informatie van de gemeente Utrecht. Als geen ander weet jij welke dreigingen er zijn en kun je deze vertalen naar risico's die de gemeente en haar inwoners lopen. Solliciteer nu!

[Lees meer](#) 



## Vacature



### Cybersecurity Trainer / Streamer

Toe aan een nieuwe nieuwe job waarmee je het verschil maakt? In de Certified Secure trainingen laat je deelnemers zien hoe actuele kwetsbaarheden structureel verholpen worden. Ook werk je actief mee aan de ontwikkeling van onze gamified security challenges. Bij het maken van challenges kom je telkens nieuwe technieken tegen, van Flutter tot GraphQL, van Elastic Search tot Kubernetes.

[Lees meer](#) 

## Security.NL - X

10-01-2024 door Redactie

Ach, elk automatiseringsbedrijfje noemt zich tegenwoordig al IT dienstverlener terwijl het gewoon veredelde computermannetjes zijn....

Altijd meteen op de hoogte van het laatste security nieuws? Volg ons ook op X!

[Lees meer](#)

11-09-2024, 21:56 door Anoniem

[Reageer met quote](#)



*Door Anoniem:* Kortom: knoeien kost max. 50k. Dan kan de rekensom gemaakt worden.

In deze branche is imago ook natuurlijk belangrijk. De kost ligt dus waarschijnlijk hoger.

Maar voor de eerste infractie - voor zover ik weet - kan je natuurlijk moeilijk een bedrijf failliet maken als rechter.

11-09-2024, 22:41 door Anoniem

[Reageer met quote](#)



*Door Anoniem:* Ach, elk automatiseringsbedrijfje noemt zich tegenwoordig al IT dienstverlener terwijl het gewoon veredelde computermannetjes zijn....

Precies, ik denk dat klanten veel kritischer moeten zijn als ze contracten met IT-dienstverleners afsluiten. Als je voor de goedkoopste lokale computershop op de hoek kiest, dan moet je niet verwachten dat je high end beveiliging hebt....

11-09-2024, 22:45 door Anoniem

[Reageer met quote](#)



*Door Anoniem:* Goh, extern inhuren is toch altijd beter . Gnif gnif. Die kleine mkb ict bedrijfjes hebben de kennis gewoon niet om dit soort zaken gewoon goed op orde te hebben. Als je met een paar man een 'ict bedrijf' runt dan is er vaak gewoon niet kennis of mankracht genoeg voor dit soort zaken OF het moet allemaal zo goedkoop mogelijk ( van de klant en voor de dienstverlener zelf ).

Wat zit jij nu te gniffelen? Zowel inhuur en/of vast personeel kan een ramp zijn.

12-09-2024, 08:09 door Anoniem

[Reageer met quote](#)



Met een wurgcontract en schadevergoedingen zal een dienstverlener alleen instemmen als er geen enkele change meer word uitgevoerd zonder gigantische doorlooptijd, papierwinkel en goedkeuringscarrousel.

12-09-2024, 12:41 door Anoniem

[Reageer met quote](#)



Wel bijzonder dat er door de leverancier meerdere keren de zwakheden zijn aangegeven, whitelisting, Vlan, verouderde server wachtwoorden etc. en dat dan alsnog de leverancier aansprakelijk is?

12-09-2024, 12:53 door Anoniem

[Reageer met quote](#)



*Door Anoniem:*

*Door Anoniem:* Kortom: knoeien kost max. 50k. Dan kan de rekensom gemaakt worden.

In deze branche is imago ook natuurlijk belangrijk. De kost ligt dus waarschijnlijk hoger.

Maar voor de eerste infractie - voor zover ik weet - kan je natuurlijk moeilijk een bedrijf failliet maken als rechter.

Ik denk niet dat "ze mogen er niet failliet van gaan" een overweging is.

Als de schade aantoonbaar, en de aansprakelijkheid ervoor ook - dan mag (en moet) de volle mep bij de aansprakelijke gelegd worden. Ook als ze daar failliet van gaan. (voor prive-personen - schuldsanering in) .

Jammer natuurlijk voor het slachtoffer als de aansprakelijke de schade inderdaad niet \_kan\_ betalen , maar de claim kan toegewezen worden.

Niet voor niks dat ze daar (in de bouw ) aparte BV voor oprichten voor een project . Die kan ploffen en dan is dat de claim limiet.

12-09-2024, 13:50 door [wim-bart](#)

[Reageer met quote](#)



Zo een beetje iedere minimale basisregel voor beveiliging en goed beheer is geschonden. Ik vraag mij af hoe dit bedrijf zijn dienst verlening goed kon uitvoeren.... O ja, natuurlijk doordat alles open stond voor iedereen, kan iedereen er bij.

Heb niks gehoord over end user devices. Maar ik verwacht dat dit net zo slecht was.

Dit soort "IT bedrijven" moeten gewoon out of business gaan. Zo een slechte naam voor de business want er zijn meer dan genoeg bedrijven welke het wel goed doen.

RDP open naar Internet, dat was in 2014 al not done (eigenlijk nooit done)

Een enkel Admin wachtwoord voor alle servers. Sterker nog, dit is al jaren not done. Je hebt oplossingen als CyberArk hiervoor. En een domein account met local Administrator rechten is ook al eeuwen not done.

Geen updates, je kan dat toch niet zeggen zonder tranen in de ogen.

Server die al uit moest staan? Waar is lifecycle management? Hebben ze wel een CMDB

Dit soort bedrijven zal nooit ISO, SOC2, NIST gecertificeerd worden.

12-09-2024, 14:24 door Anoniem

[Reageer met quote](#)



*Door Anoniem:* Wel bijzonder dat er door de leverancier meerdere keren de zwakheden zijn aangegeven, whitelisting, Vlan, verouderde server wachtwoorden etc. en dat dan alsnog de leverancier aansprakelijk is?

Nou dit dus!

Reageren

Ondersteunde bbcodes

Je bent niet [ingelogd](#) en reageert "**Anoniem**". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt **niet direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt

kun je [hier](#) direct een account aanmaken. Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.



Nieuwe code

Herhaal code:

Preview

Reageren



Over Security.NL

Huisregels

Privacy Policy

Adverteren

© 2001-2024 Security.nl - The Security Council

 Twitter  RSS