# Hoe cyberinsurance bij kan dragen aan betere ICT-mores in zorgland


**Op Twitter verscheen op 2 september 2019 een duidelijke waarschuwing van Matthijs R. Koot, cyberexpert werkzaam bij Secura B.V., een cybersecurity-bedrijf. Het gaat om een zeer recent bekend geworden kwetsbaarheid van bepaalde VPN-diensten, die o.a. in gebruik zijn bij onze overheid en andere instituties. Een kwetsbaarheid die inmiddels hersteld is door een "patch", maar die wel de vraag opwerp of alle gebruikers van VPN-diensten wel adequaat die patch installeren. In zijn blog van 1 september geeft Koot een nauwkeurige beschrijving en wijst daarin een passant op een zeer recent artikel van de juriste Nynke M. Brouwer.** Zij werkt als advocaat bij Dirkzwager advocaten & notarissen en als buitenpromovenda verbonden aan het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit. Zij publiceerde in het magazine Aansprakelijkheid, Verzekering & Schade, het artikel 'Vlijt en naarstigheid' in een digitale wereld: eigen schuld en beredding in de context van de cyberverzekering' ( AV&S 2019/23, afl. 4). Het lijkt een wat droge materie om als niet-jurist te lezen, maar er staan zeer goede observaties en conclusies in. Daarbij denk ik aan hoe in de cyberinsurance verzekeraars bij kunnen dragen aan betere ICT-mores bij hun klanten. Ik kijk in mijn artikel nu naar een deel van die klanten: zorgaanbieders met hun ICT-systemen.

## Zeer urgent probleem

Zoals in de aanhef vermeld gaat het probleem met de kwetsbaarheid zeer veel diensten en bedrijven aan. De

kwetsbaarheid zit in Pulse Connect Secure SSL VPN's in de Nederlandse IP-adresruimte. Een anonieme niet-ingelogde aanvaller kan op afstand ermee willekeurige bestanden uitlezen. Er is inmiddels een patch voor. Daarop is echter door nog lang niet alle bedrijven en instituties die gevaar lopen adequaat geacteerd met het installeren van de inmiddels 2 maanden oude patch. In de Nederlandse IP-adresruimte blijkt het om totaal 537 IP-adressen te gaan waarvan er op de ochtend van 2 september 2019 nog 300 kwetsbaar zijn.

## Sectoren

De initiële lijst van kwetsbare systemen bevat systemen van:

- Rijksoverheid
- lokale overheden
- luchtvaartsector
- beursgenoteerde bedrijven met intellectual property
- defensie-industrie
- onderwijssector, waaronder een universiteit en een hogeschool
- financiële sector: meerdere banken, verzekeraars, belasting- en administratiekantoren
- ICT-bedrijven: meerdere bekende/grote namen (met o.a. Defensie als klant) en enkele ICT-beveiligingsbedrijven
- havenbedrijven
- petrochemische industrie
- **zorgpartijen: zorgaanbieders en nationale zorg-ICT (WJJ: Ja, welke zouden dat zijn?)**
- enkele kleinere ISPs en telecomproviders
- […meer…]

## Actie

Het voorval is gemeld aan cybersecurity-partijen en toezichthouders in Nederland maar het aantal ongepatchte systemen is nog hoog. Op het moment van dit artikel ruim meer dan de helft nog. Bedrijven en instellingen en zeker

zorginstellingen/zorgaanbieders die gebruik maken van VPN-verbindingen dienen zich af te vragen of ze daarvoor Pulse Connect gebruiken en zo ja of de benodigde patch geïnstalleerd is. Indien men wil laten testen of men at risk is kan contact opgenomen worden met matthijs.koot@secura.com van cybersecurity-bedriijf Secura B.V. Door een simpele controle van hostnaam en/of IP/adres kan dan snel een antwoord gegeven worden.

## Eigen schuld en bereddingsplicht

Aan de hand van de verzekeringstechnische leerstukken 'eigen schuld' en 'de bereddingsplicht' gaat juriste mr. Nynke Brouwer in haar in de aanhef genoemde artikel diepgaand in op de datgene wat van de klant met een ICT-verzekering en van de verzekeraar verwacht kan en mag worden. Het begrip eigen schuld betekent dat verzekeraars geen schade vergoeden die is veroorzaakt door opzet of roekeloosheid van de verzekerde (artikel 7:952 BW). De bereddingsplicht houdt in dat de uitkeringsplicht van de verzekeraar (mede) bepaald wordt door het handelen van de verzekerde zelf. De verzekerde moet, wil hij recht hebben op (volledige) uitkering voor zijn schade, bijzondere maatregelen treffen om onmiddellijk dreigend gevaar zoveel mogelijk af te wenden of de ontstane schade zoveel mogelijk te beperken.

## Cybersecurity

In het artikel maakt Nynke Brouwer duidelijk dat verzekeraars het begrip 'cybersecurity' in vragenlijsten aan klanten en in de te noemen voorwaarden in polisbladen niet eenduidig opstellen. Gezien de voortschrijdende techniek en het bekend worden van nieuwe kwetsbaarheden in hard- en software is het ook lastig om tot in detail de te nemen maatregelen vast te leggen.

## Constatering

Brouwer constateert op pagina 122 van haar artikel:

*Een enkele uitzondering daargelaten, worden deze maatregelen echter weinig geconcretiseerd. Binnen hoeveel dagen een patch of update moet worden geïmplementeerd, is dus aan de inschatting van de verzekerde zelf. Ik vraag mij af of dit niet een gemiste kans is voor zowel verzekeraars zelf als de maatschappij in bredere zin. Grote incidenten zoals Wannacry en NotPetya tonen aan dat het belang van zo snel mogelijk patchen zeker niet moet worden onderschat. Ter verhindering van de kwetsbaarheid die Wannacry mogelijk maakte had Microsoft al twee maanden eerder een patch uitgegeven, maar nog niet alle bedrijven en organisaties hadden deze geïnstalleerd. Dit lijkt vrij eenvoudig te ondervangen door in de polisvoorwaarden of – zou dit meer maatwerk betreffen – op het polisblad een termijn voor het installeren van patches op te nemen. Hetzelfde geldt voor de algemeen gestelde vraag naar back-ups. De aanvraagformulieren geven niet aan hoe vaak deze back-ups moeten worden gemaakt en waar dat wel het geval is, zijn de verschillen groot: dagelijks, wekelijks, maandelijks.*

## Disciplinerend

Waar in zorginstellingen het regelmatig installeren van updates en patches van de software nogal eens het stiefkind is, kunnen cyberverzekeraars een broodnodige disciplinerende werking  gaan hebben op het gedrag van verzekerden. Geen uitkering van de verzekering bij cybercalamiteiten als de zorgverlener/ zorginstellingen niet aan zijn zorgplicht ten aanzien van de eigen hard- en software heeft voldaan. Kortweg dus: wie klant is bij een cyberverzekeraar en vier maanden lang een kritieke beveiligingspatch op een internet-facing systeem niet installeert hoeft bij een compromittering waarschijnlijk niet te rekenen op een uitkering. De in dit artikel genoemde kwetsbaarheid met  Pulse connect Secure SSL

VPN is daar een voorbeeld van.

Het zou een welkome vorm zijn van het brengen van druk op de ketel zijn.

W.J. Jongejan, 3 september 2019

Afbeelding van Andrew Martin via Pixabay