DE TIJD

# Wannacry: blitzkrieg van een computerworm

15 mei 2017 22:39

Pieter Haeck
Dorien Luyckx

**Een cyberaanval op ongeziene schaal gijzelde de afgelopen dagen meer dan 200.000 computers in 150 landen. Het legt de vinger op de soms lakse digitale beveiliging.**

Britse ziekenhuizen, Chinese en Russische overheidsinstellingen, de autofabrikanten Nissan en Renault, de pakjesreus FedEx en China's grootste olieproducent PetroChina. Enkele groten van deze aardbol stonden dit weekend in hun blootje als slachtoffer van een cyberaanval zonder weerga. Hun computersystemen waren niet meer bereikbaar door 'ransomware', een computervirus dat computers gijzelt met alle bestanden en systemen incluis. Wereldwijd waren meer dan 200.000 computers in 150 landen getroffen, schat de Europese politiedienst Europol.

**Wat is het probleem?**

Via 'phishingmails', mails die echt lijken maar eigenlijk door criminelen ontworpen zijn om mensen te laten klikken op besmette bestanden of links, drong het 'WannaCry'-virus binnen in computers wereldwijd. Dat virus is een vorm van ransomware, een computerbesmetting die zo geprogrammeerd is dat al uw bestanden of systemen 'op slot' gaan. De criminelen geven alles opnieuw vrij na betaling van 300 dollar in de virtuele munt bitcoin.

Gisteravond hadden de criminelen iets meer dan 55.000 dollar op zak. Dat lijkt weinig, maar met ransomware plukken criminelen alleen laaghangend fruit, klinkt het in de sector. 'Ransomware is nog zo vriendelijk om te zeggen dat je een probleem hebt', legt Erwin Geirnaert van het cybersecuritybedrijf ZionSecurity uit. Een oplettende onderzoeker heeft de aanval voorlopig afgeslagen, maar nieuwe, lastiger af te weren varianten zijn altijd mogelijk.

**Hoe is het zover kunnen komen?**

De Amerikaanse geheime dienst NSA had al enige tijd weet van een kwetsbaar punt in oudere versies van Windows, het besturingssysteem van Microsoft. De achilleshiel was het SMB-protocol, waarmee computers bestanden uitwisselen. De NSA buitte het Microsoft-foutje uit voor haar eigen profijt om aan data- en informatieverzameling te doen.

Maar een groep genaamd 'Shadow Brokers' ging aan de haal met een deel van de gereedschapskoffer van de NSA en gooide die online. In februari was er een eerste, weliswaar beperkte, WannaCry-golf. Microsoft kreeg lucht van de dreiging en zette al op 14 maart een 'patch', een soort van pleister voor

de digitale wonde, online om het lek te dichten. Toch kon de tweede WannaCry-golf dit weekend nog flink huishouden. 'Veel bedrijven zijn niet mee met de jongste updates van Windows', duidt Danielle Jacobs, directeur van Beltug, de vereniging van zakelijke ICT-gebruikers.

**Hoe kon het zo snel woekeren?**

Ransomware is niet nieuw. Wel nieuw was de manier waarop WannaCry zich verspreidde. Dat heeft veel te maken met het SMB-protocol, waar het lek in zat. Om bestanden te kunnen delen over een netwerk staat de 'knop' van dat protocol per definitie aan. Er is dan maar één besmette computer nodig om een heel netwerk te kunnen aanvallen. 'Bedrijven beschikken vaak wel over firewalls, waarmee ze zich van het verkeer van buitenaf beschermen', stelt Geirnaert. 'Nu was er maar één besmet punt nodig.' Zodra de worm binnen was geraakt, vrat hij zijn weg door het systeem.

**Hoe beveiligt u zich?**

Voorlopig is het WannaCry-virus onschadelijk gemaakt door een opmerkzame onderzoeker. Hij maakte het virus wijs dat als het 'actief' werd, het zich eigenlijk in een testomgeving bevond. Daardoor valt het virus niet aan.

Toch moet u nog steeds op uw hoede zijn. Als uw computers nog draaien op een ouder besturingssysteem dan Windows 10 moet u zo snel mogelijk de patch 'MS17-010' downloaden en installeren. Een upgrade naar Windows 10, waarin het lek al gedicht is, is ook een optie. Voorts moet u opletten met mails die er verdacht uitzien.

'Dit virus zal nog vele jaren gebruikt worden in tal van varianten', zegt Bart van den Bosch, hoofd informatica van het UZ Leuven, een van de grootste ziekenhuizen van dit land. De Leuvense systemen bleven overeind, maar Van den Bosch maakt zich geen illusies. 'Het virus zal hier ook aan de deur hebben gestaan.'

Ook in het UZ Gent weerde de firewall elke aanval af. Het parkeerbedrijf Q-Park België en de Antwerpse pensioendienst hadden minder geluk. Klanten konden zonder te betalen de Q-Park-parking aan het Brusselse Zuidstation verlaten. De Antwerpse pensioendienst moest enkele afspraken annuleren tot de computers van het personeel gecontroleerd waren.

**Wat zegt het over onze digitale veiligheid?**

'Dit had voorkomen kunnen worden', vindt Koen Maris, technologiedirecteur van het cybersecuritybedrijf Atos. IT'ers in bedrijven zijn wel op de hoogte van kwetsbaarheden, maar door budgettaire krapte of een povere opvolging kwamen er amper oplossingen. 'Ik krijg de jongste maanden gevoelig meer vragen over ransomware, dus IT'ers beseffen dat er snel oplossingen nodig zijn. Maar de rest van het bedrijf volgt niet altijd', zegt Maris.

Mee zijn met de laatste updates is vooral voor openbare instellingen, zoals ziekenhuizen, overheidsdiensten, scholen en universiteiten geen evidentie. 'Ik ga niet beweren dat ze er losjes mee omgaan, maar soms is het kiezen tussen snel updates doorvoeren, waarbij er iets kan fout lopen, of blootge-

steld zijn aan allerlei kwetsbaarheden', zegt Frank Staut, technologiedirecteur van het Belgische cybersecuritybedrijf SecureLink.

Deze aanval is hoe dan ook een uitstekende vorm van bewustmaking, menen experts. Dat was ook nodig, want het aantal slachtoffers van ransomware zat de jongste tijd in stijgende lijn.

Bron: De Tijd