TEKST: REMKO EBBERS **FOTO:** MARGOT HARTFORD/GETTYIMAGES

JA MAAR MIJN KAT LAG OP HET TOETSENBORD

EN 5 ANDERE SLAPPE EXCUSES OM NIETS AAN COMPUTERBEVEILIGING TE DOEN

Na Petya Wrap en WannaCry is de hele wereld toch wel gewaarschuwd? En houdt iedereen zijn computers veilig? Nou... Je kunt echt nooit voorzichtig genoeg zijn als het om cybersecurity gaat. Want criminelen vinden gaten in je beveiliging zo. Dit kun je doen om dat te voorkomen.

Op 27 juni 2017 hield de wereld even de digitale adem in. Het gijzelprogramma Petya Wrap vloog over de wereld. Een kleine anderhalve maand na de aanval met WannaCry-ransomware. Half juni waarschuwde het Slowaakse beveiligingsbedrijf ESET ook voor Industroyer, een virus dat al actief was in Oekraïne en onder andere energiecentrales, sluizen en transportsystemen kan platleggen. Kenners denken dat de gevaren groter zijn dan bij Stuxnet uit 2010. Dat had als doel het nucleaire systeem van Iran aan te vallen. WannaCry was gericht op een fout in het oude Windows XP. Waren er nog mensen die XP gebruikten? Zeker wel, volgens Europol heeft de cyberaanval tweehonderdduizend slachtoffers gemaakt in minstens 150 landen. Petya Wrap trof nog eens duizenden bedrijven en particulieren, waaronder – in Nederland – APM Terminals en TNT. Maar hoe kun je nou voorkomen dat je zelf slachtoffer wordt? Vijf excuses die je dan nooit moet gebruiken:

#1 'MIJN BEDRIJF IS VEEL TE KLEIN OM INTERESSANT TE ZIJN VOOR HACKERS EN SPIONNEN'

Je bent niet gauw te klein. Wie bij een groot bedrijf binnen wil komen, kan dat proberen via kleinere toeleveranciers. En trouwens, alleen al een bestand met adressen, creditcardgegevens of rekeningnummers is interessant. Creditcardgegevens leveren minstens 50 dollarcent tot 2,50 dollar per kaart op, medische patiëntendossiers 10 tot 20 dollar per stuk. Zelfs de Belgische professor Jean-Jacques Quisquater, een internationaal expert in het beveiligen van data, werd in 2014 gehackt. En gijzelsoftwaremakers zijn sowieso niet kritisch. Zij vragen vaak relatief kleine bedragen zodat getroffenen makkelijk betalen om overal snel vanaf te zijn. Dus *size does not matter*.

#2 'IK HEB EEN APART PROTOCOL VOOR PATCHES, ANDERS GOOI IK MIJN OUDE SYSTEMEN IN DE WAR'

'Wij hebben een apart protocol voor het installeren van digitale kurken in een beveiligingslek (patches dus)', wordt wel gezegd. 'Zomaar alles installeren brengt onze oude systemen in de war.' Mooi. Maar maak er geen managementproject van. Een bedrijf dat zes weken nodig heeft om een 'digitale kurk' voor een beveilingslek te testen, dan zes weken gebruikt om het script te maken dat de reparatie aanpast op de oude systemen en tot slot zes weken de tijd neemt om het nieuwe systeem uit te rollen, laat de hacker/het virus achttien weken lang zijn gang gaan. Waargebeurd verhaal. Dat moet je dus nooit doen. Haal er dan desnoods een specialist bij, maar zorg in elk geval altijd dat je systeem totaal *up-to-date* is.

#3 'WIJ MOETEN DEZE BESCHERMINGSFUNCTIE WEL UITZETTEN, WANT HET CONFLICTEERT MET DE AANSTURING VAN EEN VAN ONZE MACHINES'

Als je it'er zoiets zegt en jij gelooft dat, bent je echt een sukkel. Omdat een apparaat dat aan jouw netwerk zit of jouw boekhoudprogramma foutmeldingen stuurt, ga je toch geen digitaal beschermingspakket (deels) uitschakelen voor het hele bedrijf? Neem contact op met de leverancier en zorg voor een maatwerkoplossing voor die ene machine of dat ene pakket. Het kost inderdaad wat, maar dan blijft je bedrijf wel digitaal op slot. En dat wil je niet alleen zelf graag, maar je klant ook.

Computer 'gegijzeld'? Niet betalen, wel direct naar de politie en je contactpersoon van je cybersecuritypakket bellen

#4 'JA MAAR, IK HEB TOCH ALLES OP EEN BACK-UP'

Zeker weten? Staat die back-up ook los van het systeem? Want menig back-up raakt meteen geïnfecteerd als de pc of de server dat is, omdat-ie permanent verbonden is. En een advies van de specialist: niet steeds dezelfde back-upschijf/stick gebruiken. Raakt die ene namelijk toch besmet tijdens zijn 'werk', ben je alsnog alles kwijt.

#5 'IK HEB MIJN MENSEN AL EENS VERTELD DAT ZE NIET ZOMAAR OVERAL OP MOETEN KLIKKEN'

Vertel het gerust nog eens. En over een half

OOIT GEDACHT: 'ACH MIJN BEDRIJF IS TE KLEIN VOOR CRIMINELEN'? THINK AGAIN

KOEN VAN WEEL/ANP

Wat moet je doen als je computer is gegijzeld? 6 Simpele stappen

STAP 1.
Bedenk wat er gebeurt. Is er een virus actief, een trojan, spionagesoftware of is het juist ransomware?

STAP 2.
Kijk bij gijzelsoftware op de site nomoreransom.org om te zien of jouw variant al bekend is;

STAP 3.
Bel zo snel mogelijk de contactpersoon van je cybersecurity-pakket;

STAP 4.
Trek minstens een dag uit om het probleem te verhelpen. En hou er rekening mee dat het oplossen van de problemen die door de aanval zijn ontstaan, ook zomaar een week kan duren;

STAP 5.
Doe altijd aangifte bij de politie. Mocht je niet voorbij de 'afpoeierdesk' van het plaatselijke politiebureau komen: kijk dan op nomoreransom.org. Daar staat een kant-en-klare handleiding. Plus wat je moet meenemen om aangifte te doen;

STAP 6.
Dit klinkt misschien gek, maar: stuur onmiddelijk alle medewerkers (opnieuw) op cyberveiligheidstraining!

jaar nog eens. Volgens de experts van beveiligingsbedrijf Kaspersky ontstaan de meeste infecties gewoon via een foute mail aan een medewerker die wordt geopend. Een bank stuurde twee maanden na een bedrijfsbrede training over *cybercrime* en *phishing* een anonieme testmail om te kijken of de lesstof was blijven hangen. De helft van de werknemers klikte zonder meer op de link. Zie het maar als EHBO- of BHV-training die je ook regelmatig moet herhalen.

EN TOT SLOT: DOE ALTIJD AANGIFTE BIJ DE POLITIE

Ach, aangifte doen kost tijd en haalt niets uit? Onzin, zeggen experts van Kaspersky. Althans: doe altijd aangifte. Zo weet de politie tenminste waar de klappen vallen. Bij het grootbedrijf of winkels? In Groningen of Zeeland? Bij metaalbedrijven of administratiekantoren? Aan de hand daarvan kan de politie mensen inzetten en tijd vrijmaken waar het nodig is. En om het wat makkelijker te maken: er staat op de website nomoreransom.org een kant-en-klare handleiding om de 'afpoeierdesk' van het plaatselijke politiebureau te weerstaan. ◘

Met dank aan onder anderen Remco de Groot (head of customer support) en Jornt van der Wiel (security researcher en ransomware specialist) bij Kaspersky