29 jun 2017 -12:25

Cyberaanval Petya ransomware: CERT.be brengt rapport uit

Een cyberaanval met Petya ransomware legde op dinsdag 27 juni opnieuw heel wat computernetwerken plat. In België is de impact eerder beperkt, maar wereldwijd zijn de gevolgen groot. Van 3 bedrijven die CERT.be een melding deden, kunnen we bevestigen dat het om Petya ransomware gaat. Wij hebben vandaag geen nieuwe meldingen ontvangen.

Uiteindelijk werd een handvol multinationals met een zetel in België het slachtoffer van deze cyberaanval. Voor hen is de schade allicht aanzienlijk. Bedrijven die de adviezen van CERT.be na de uitbraak van WannaCry een maand geleden goed opvolgden, bleken beter beschermd tegen deze aanval.

Patient zero

Voor de uitbraak van het virus kijken we naar Oekraïne. Toen de Oekraïense overheden dinsdagochtend aan de slag gingen, gebeurde er een automatische update van MEDoc, een boekhoudingsoftware. We vermoeden dat deze update de besmetting veroorzaakte. De besmetting verspreidde zich razendsnel binnen de overheidsdiensten en nadien ook bij hun toeleveranciers.

WannaCry

Er is gelijkenis met het WannaCry virus, dat afgelopen maand wereldwijd computernetwerken kon besmetten. Petya maakt immers gebruik van dezelfde kwetsbaarheden als WannaCry. Bij WannyCry werd de ‘killswitch’ snel gevonden en stopte de besmetting. Bij Petya is er een onbevestigde ‘killswitch’. De besmettingen lijken intussen wereldwijd af te nemen.

Hebben we erger voorkomen?

De inspanningen van CERT.be na de uitbraak van WannaCry lijken effect te hebben. CERT.be voerde een informatie- en sensibiliseringscampagne om besmettingen met ransomware te voorkomen. Omdat vele bedrijven actie ondernamen na WannaCry, waren ze daarom beter gewapend tegen deze nieuwe cyberaanval.

CERT.be volgt de situatie nog steeds permanent op. Bedrijven die slachtoffer zijn, kunnen dit melden op cert@cert.be.

Wij raden in elk geval aan om deze cybercriminelen niet te betalen. Petya is eerder een wiper die gegevens vernietigt en niet doodzakelijk uit is financieel gewin.

Alle technische adviezen worden beschreven in het rapport van CERT.be dat later op de dag verschijnt.

Beter gewapend zijn tegen ransomware? Lees hier.

Over het CERT.be

CERT.be is het federal cyber emergency team, dat als neutrale specialist in internet –en netwerkveiligheid

bedrijven ondersteunt bij het coördineren bij cyberbeveiligingsincidenten, adviseert om een oplossing te vinden wanneer er zich cyberbeveiligingsincidenten voordoen en hen bijstaat om deze beveiligingsincidenten te voorkomen.

Over het Centrum voor Cybersecurity België

Het Centrum voor Cybersecurity België (CCB) is het nationale centrum voor cyberveiligheid in België. Het CCB stelt tot doel het superviseren, het coördineren en het waken over de toepassing van de Belgische strategie betreffende cyberveiligheid. Door het optimaliseren van de informatie-uitwisseling zullen de bevolking, de bedrijven de overheid en de vitale sectoren zich gepast kunnen beschermen.
www.ccb.belgium.be

De nationale sensibiliseringscampagne rond cyberveiligheid die in oktober door het Centrum voor Cybersecurity België en het CERT wordt georganiseerd heeft tot doel de Belgische burger waakzaam te maken voor verdachte e-mails.

Contact pers

Katrien Eggers
0485765336

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - momenteel in verlof Eggers - momenteel in verlof
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be