Cyberaanval legt wereldwijd honderden bedrijven plat, nog geen weet van Belgische slachtoffers
Een wereldwijde cyberaanval heeft al honderden bedrijven getroffen. Hackers hebben een valse beveiligingsupdate gestuurd naar bedrijven in onder meer de Verenigde Staten, Zweden en Nederland. Bij ons zijn er nog geen gevallen bekend, maar bedrijven kunnen zich wel nog beschermen door de geïnfecteerde software uit te schakelen.

Koen Braeckman
za 03 juli

De software waarover het gaat is het VSA-programma van het bedrijf Kaseya, nota bene een softwarebedrijf dat zich specialiseert in cyberveiligheid. Dat meldt Het Nieuwsblad op zijn site. De hackers – vermoed wordt dat het om Russen gaat, maar dat is nog niet zeker – hebben vrijdagavond eerst naar Amerikaanse bedrijven een valse beveiligingsupdate gestuurd.
Wie de update installeerde, kreeg de melding dat het computersysteem geïmpacteerd was en dat er losgeld moest betaald worden. De bedragen kunnen in de miljoenen dollars lopen. De cyberaanval zit intussen ook al in Nederland en in Zweden, waar 800 winkels van de COOP-warenhuisketen de deuren moesten sluiten. Het is heel belangrijk om die systemen nu zo snel mogelijk tijdelijk uit te schakelen.
Miguel De Bruycker, Centrum voor Cybersecurity België
Het Centrum voor Cybersecurity België heeft nog geen weet van bedrijven bij ons die getroffen zijn, maar dat kan met het weekend te maken hebben. Het Centrum heeft wel al een waarschuwing uitgestuurd. Wie de valse update krijgt, moet het programma meteen uitschakelen. Miguel De Bruycker van het Centrum voor Cybersecurity: "Zolang het systeem niet is misbruikt om ransomware te verspreiden, is de impact beperkt. Maar het is heel belangrijk om die systemen nu zo snel mogelijk tijdelijk uit te schakelen in afwachting van verdere richtlijnen van de leverancier."
Volgens Het Nieuwsblad is de cyberaanval het werk van het Russische hackerscollectief REvil. Volgens Miguel De Bruycker is dat "nog niet 100 procent zeker". Als het de Russen zijn, zijn ze alleszins niet aan hun proefstuk toe. Ze zouden ook achter de grote cyberaanval zitten die een maand geleden het internationale vleesbedrijf JBS platlegde.
Een Antwerpse ICT-dienstverlener meldt intussen dat hij getroffen is door een cyberaanval. Daardoor zijn de gegevens van een vijftigtal klanten geblokkeerd, vooral KMO's. Maar het is nog niet duidelijk of het om dezelfde daders gaat als in de VS, Nederland en Zweden.

Hanne Decré
ma 05 juli
Vermoedelijke hackers achter de grote cyberaanval eisen maar liefst 70 miljoen dollar om bestanden opnieuw vrij te geven.

De hackers die vermoedelijk achter de grote cyberaanval van dit weekend zitten, eisen 70 miljoen dollar om de gegevens opnieuw vrij te geven. Dat staat te lezen in berichten op het dark web**.** Honderden bedrijven van over de hele wereld zijn getroffen.

Maar liefst 70 miljoen dollar eisen de hackers die waarschijnlijk achter de grote cyberaanval van afgelopen weekend zitten. Voor dat geld zou de groep een universele sleutel vrijgeven waardoor de getroffen bedrijven hun bestanden opnieuw krijgen. Volgens de hackersgroep zelf zijn er een miljoen systemen geïnfecteerd, al is er nog geen duidelijkheid over het precieze aantal.

Hoe gingen de hackers te werk?

De hackers drongen binnen bij Kaseya, een Amerikaans softwarebedrijf dat gespecialiseerd is in cyberveiligheid. Eens binnen stuurden de hackers vrijdagavond een valse beveiligingsupdate naar de klanten van Kaseya. Eens die valse update geïnstalleerd was, kregen de bedrijven een bericht dat hun computersysteem geïmpacteerd was en dat ze miljoenen zouden moeten betalen om hun bestanden opnieuw in handen te krijgen.

Op die manier werden honderden bedrijven over de hele wereld lamgelegd, onder meer in de Verenigde Staten, het Verenigd Koninkrijk, Colombia, Zuid-Afrika, Zweden en Nederland. Zo moesten honderden winkels van supermarkt Coop zaterdag sluiten omdat de kassa's offline waren - een gevolg van de aanval. Het Witte Huis had dit weekend te kennen gegeven dat het contact zou opnemen met de slachtoffers "om hulp te bieden".

Zit de Russische groep REvil hier achter?

De grote vraag is nu wie er achter de grote cyberaanval zit. Er wordt in de richting gekeken van REvil, een hackersgroep die aan Rusland gelinkt wordt. De miljoeneneis werd gepost op een blog die de groep vaak gebruikt. REvil is alleszins niet aan zijn proefstuk toe. Zo zouden ze ook achter de grote cyberaanval zitten die vorige maand het internationale vleesbedrijf JBS platlegde. JBS zou uiteindelijk 11 miljoen dollar betaald hebben.

Bron: VRT Nieuws