Het CCB waarschuwt: Laat België niet lamleggen door ransomware!

Door Andries Bomans, Katrien Eggers
Gepubliceerd op 19/09/2019

Ransomware is bezig aan een opmars, maar bescherming is mogelijk.

Hoewel ze al dateren van 2017 en 2018 staan WannaCry en NotPetya nog vers in het geheugen gegrift. Het was de eerste keer dat in ons land de gevolgen van een wereldwijde aanval met ransomware gevoeld werden. Begin dit jaar werden we opgeschrikt door een nieuwe familie van ransomware, Anatova genaamd. En ook de Amerikaanse autoriteiten vrezen een aanval tijdens de verkiezingen van 2020. Ransomware is zonder meer aan een opmars bezig.

Wie wordt geviseerd door ransomware?

Iedereen kan het slachtoffer worden van ransomware: van gamers tot beoefenaars van zelfstandige beroepen, ziekenhuizen, grote bedrijven en de overheid. In Frankrijk legde een ransomware recent maar liefst 120 ziekenhuizen plat. Eerder dit jaar was een Belgisch ziekenhuis ook al slachtoffer. In haar jaarverslag 2018 merkte ENISA op dat de gezondheidssector in het bijzonder wordt geviseerd door dergelijke aanvallen. Ook in België haalden verschillende gevallen van ransomware dit jaar de pers.
Maar dit is het topje van de ijsberg. Particuliere slachtoffers geven een dergelijke aanval zelden aan en ook bedrijven zijn niet happig om bekend te maken dat ze slachtoffer werden van ransomware. Naast de financiële verliezen kan ook de imagoschade aanzienlijk zijn voor een bedrijf.

Hoe je beschermen tegen ransomware?

Het goede nieuws is dat bescherming tegen ransomware mogelijk is.
Voor elke internetgebruiker:
• Het is belangrijk dat je toestellen beschermd zijn met een antivirussoftware, maar daarnaast is ook specifieke bescherming tegen ransomware een must geworden. Installeer anti-ransomware, zoals Acronis Ransomware Protection, Kasperski Anti-Ransomware Tool for Business, McAfee Ransomware Interceptor (Pilot). Voor Windows 10 gebruikers: Windows Defender Antivirus.
• Daarnaast blijft het belangrijk om valse berichten op tijd te herkennen en regelmatig updates uit te voeren op al je systemen.
• Maak ten slotte regelmatig back-ups voor het geval je toch slachtoffer wordt.
Voor bedrijven en organisaties:
De aanbevelingen voor elke internetgebruiker zijn natuurlijk ook belangrijk voor bedrijven en organisaties, maar hen raden we aan om nog een stap verder te gaan.
• Voor KMO's en zelfstandige beroepen kan een End-Point bescherming zoals lijst hierboven voldoende zijn. Voor grote bedrijven is een gespecialiseerde business anti-ransomware oplossing aanbevolen.
• Zorg voor een business continuity and recovery plan met een getest backup-systeem
• Zorg dat je organisatie voorbereid is op een cyberaanval. Bekijk onze webinar: https://www.youtube.com/watch?v=-cHcTidmT1Y&feature=youtu.be
• Laat je IT security architecture & policy nakijken door een specialist. (inclusief het beleid rond patching, user training, network segmentatie, etc.)
• Maak werk van een cybersecurity strategie. Lees hier hoe je dit aanpakt: https://cyberguide.ccb.belgium.be/nl

Ransomware hoe werkt dat?

Ransomware is een virus dat wordt geïnstalleerd op een toestel zonder dat de eigenaar daarvoor toestemming gaf. Het gijzelvirus houdt het toestel en de bestanden gegijzeld (geëncypteerd) en vraagt losgeld.

Contactpersoon pers:
Katrien Eggers : 0485 765 336, katrien.eggers@cert.be

Documenten in bijlage:

- Ransomware_2019_NL.pdf (1397.6Kb)

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
http://www.ccb.belgium.be

Contacten
Andries Bomans <andries.bomans@ccb.belgium.be>
Verantwoordelijke communicatie
+32 471 66 00 06
Katrien Eggers <katrien.eggers@cert.be>
Communicatieverantwoordelijke
+32 485 76 53 36