15 jan 2021 -09:26

Centrum voor Cybersecurity België trekt lessen uit cyberaanval op Amerikaanse overheidsdiensten, de SolarWinds case

Gisteren hield het Centrum voor Cybersecurity België haar QCTR event. Een evenement dat elk kwartaal de belangrijkste cyberdreigingen van dat moment door experts laat bespreken. De online editie lokte 1300 geïnteresseerden uit meer dan 50 landen. Dit is een record en uniek voor België. Het zal niet verbazen dat de SolarWinds-case op het programma stond. Deze aanval op Amerikaanse overheidsdiensten overschaduwde alle andere actualiteiten in de USA en wordt tot op vandaag nog verder onderzocht.

SolarWinds ?

Voor wie alles gemist heeft: In december 2020 werden verschillende Amerikaanse overheidsdiensten het slachtoffer van een cyberaanval via het *Orion platform*, een softwarepakket van *SolarWinds*. Het product dat gecompromitteerd was, is een software die toelaat om systemen van op afstand te beheren. In totaal hebben 18 000 organisaties wereldwijd de kwaadaardige update geïnstalleerd en veel systemen hebben gecommuniceerd met een *Command and Control server* van de aanvallers. Verschillende organisaties hebben bevestigd dat de aanvallers verdere stappen ondernomen hebben op hun netwerk. Het gaat voornamelijk over belangrijke Amerikaanse overheidsdiensten zoals onder meer the US Treasury Department, the National Telecommunications and Information Administration (NTIA) en the National Institutes of Health (NIH).

De aanval was complex en grootschalig.

Lopen Belgische overheidsdiensten en bedrijven gevaar?

Deze software wordt over heel de wereld gebruikt, ook in België. Microsoft kon in december al 40 klanten detecteren, waarvan 1 in België. Het CCB kent niet alle Belgische klanten en kreeg tot op vandaag geen melding van een Belgisch slachtoffer. Het blijft echter belangrijk om deze dreiging op te volgen en mogelijke slachtoffers op te sporen en verder te helpen.

Wat heeft het CCB ondernomen?

Het CCB heeft deze dreiging van in het begin ernstig genomen.

"We stonden en staan voortdurend stand by om vragen van mogelijke slachtoffers te beantwoorden. Op 18/12 publiceerden we een technisch advies. We hadden meetings met verschillende Information Sharing and Analysis Centres (ISAC). Er werden rapporten gepubliceerd en gedeeld met partners via het Early Warning System (EWS). En we organiseren een event waarbij experts van onder meer FireEye en Kaspersky hun bevindingen delen om lessen te trekken voor de toekomst."

Miguel De Bruycker
Directeur Centrum voor Cybersecurity België

En wie heeft het nu gedaan?

De Amerikaanse pers wees onmiddellijk naar Russische staatshackers. Het attribueren of toewijzen van een cyberaanval is echter een zeer moeilijke zaak. Tot op vandaag hebben we geen zekerheid over wie hier achter zit.

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 - Eggers
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be