Agressieve hack SolarWinds software ook gevaar voor Nederlandse ziekenhuizen

Vermoedelijk Russische hackers van de groep Cosy Bear hebben een uiterst gesofisticeerde, agressieve, hack uitgevoerd in de SolarWinds software van Microsoft. Op 13 december 2020 kwam eerst naar buiten dat het cybersecurity-bedrijf FireEye getroffen was door een geraffineerde hack. Nog geen dag later komt het bericht dat in de Verenigde Staten een aantal overheidsinstellingen, maar ook het Witte Huis getroffen zijn door dezelfde hack. Door het binnendringen van de SolarWinds's Orion IT monitoring en management software van Microsoft konden/kunnen de aanvallers een achterdeur openzetten. Microsoft en FireEye bevestigden het. Daarmee kan men de controle overnemen en data onttrekken van systemen die SolarWinds gebruiken. Onder de gebruikers van deze software bevinden zich ook ziekenhuizen. In Nederland gaat het daarbij om meerdere ziekenhuizen. SolarWinds heeft een vestiging in Utrecht in de kantorenwijk Papendorp. Het bedrijf Adfontes Software heeft SolarWinds-software geïmplementeerd bij dozijnen ziekenhuizen en in de gezondheidszorg werkzame instellingen en bedrijven.

Adfontes Software

Op de website van dit bedrijf is het volgende te lezen:

"Adfontes Software is key IT Operations Management Software & Services vendor for dozens Hospitals & Healthcare organizations accross Benelux, over years we have set performance & diagnostic standards for market leading Chipsoft HiX, EPD's and numereous Applications being used in the

Healthcare industry with SolarWinds Application & hybrid Infrastructure management & IT Service Management software solutions. IT operations management (ITOM) software is intended to represent all the tools needed to manage the provisioning, capacity, performance and availability of computing, networking and application resources – as well as the overall quality, efficiency and experience of their delivery"

Het betekent dat ziekenhuizen die bijv. Chipsoft als Ziekenhuis Informatie Systeem(ZIS) hebben, maar ook instellingen met andere Elektronische PatiëntenDossiers(EPD'S) deze software gebruiken. Het is niet uit te sluiten dat ook ziekenhuizen met het andere in Nederland gebruikte ZIS, Epic, SolarWinds gebruiken. SolarWinds kent voor bedrijven , dus ook zorginstellingen een heel scala aan toepassingen van managementondersteuning tot het inde gaten houden van het in- en externe netwerkverkeer.

Controle/maatregelen noodzakelijk

Het spreekt vanzelf dat alle instellingen die SolarWinds software gebruiken er alles aan moeten doen om het gecompromitteerd zijn van hun systemen dienen op te sporen. Ook dienen zij maatregelen te nemen om de bedreiging te verwijderen en hernieuwde besmetting te voorkomen. Inmiddels staan er op het internet diverse aanwijzingen hoe zo iets vorm gegeven moet worden. Zo heeft FireEye gegevens vrij gegeven waarmee bedrijven die SolarWinds gebruiken. Hiermee kan men de agressieve bedreiging die zij de naam Sunburst gaven, opsporen met een update van Microsoft Defender for Endpoint. Ook publiceerde FireEye op de website GitHub een serie methoden om tegenmaatregelen te kunnen nemen tegen Sunburst, die ook met UNC2452 wordt aangeduid.

Kwetsbaarheid zorginstellingen

In het recente verleden kwamen ook andere kwetsbaarheden van zorginstellingen aan het licht. Daarbij wijs ik op de problemen met Citrix-firmware in januari 2020. Het ging daarbij om software voor apparatuur die men gebruikt om op afstand, dus bijv. vanuit huis te kunnen werken. Maar ook was er in september 2019 de problematiek met de VPN software van PulseConnect. Hoe meer zorginstellingen digitaal werken en hoe meer er sprake is van externe verbindingen met al dan niet werken op afstand des te kwetsbaarder worden de systemen.

Vijf over twaalf

Het erop vertrouwen dat het wel goed zit met de eigen systemen in zorginstellingen is geen optie. Actief dient men nu op zoek te gaan naar signalen van het gecompromitteerd zijn van de systemen. Het onderling uitwisselen binnen de zorg van kennis op dit vlak is van groot belang.

W.J.Jongejan, 15 december 2020

Afbeelding van Pete Linforth via Pixabay