

Dinsdag 23-03-2010



'Computervirus AZM wellicht veroorzaakt door onwetende medewerker'

Directeur Paul de Vlieger van het computerbeveiligingsbedrijf Com-Connect uit Horst beantwoordt enkele vragen over het computervirus dat al sinds een week het academisch ziekenhuis in Maastricht teistert. Sindsdien ligt het email-verkeer van en naar het AZM nagenoeg stil.

Wat kan er gebeurd zijn in het AZM?

Paul de Vlieger: "De meest voor de hand liggende besmetting is een gevalletje Awareness. De kans bestaat dat een niet goed geïnstrueerde medewerker een besmette usb-stick of een besmet extern opslagmedium gebruikt heeft. Wij weten niet of het AZM een zogeheten patchmanagement toepast, ofwel tijdig antivirus upgrades uitvoert."

De laatste variant van het W32/Sality virus is medio februari uitgekomen en zou dus door een up to date virusscanner onderschept moeten worden.

"Het kan natuurlijk ook zo zijn dat een medewerker via een weblink op een besmette internetpagina terecht is gekomen en niet door de security software is opgemerkt. Het Sality-virus doet daarna zelf zijn werk maar zou op een server onderschept of geblocked moeten worden door de virusscanner om verdere verspreiding tegen te gaan!"

Wat doet het virus?

"Het Sality-virus is een zogeheten file infector met trojan-eigenschappen. Dat laatste betekent dat data en of andersoortige gegevens gestolen kunnen worden. Computers kunnen traag worden net als servers. De pc's zijn met heel andere zaken bezig dan met het draaien van de normale programmatuur."

Kunnen gegevens van patiënten op straat terecht komen?

"Patiëntgegevens zullen een bepaalde vorm van encryptie bevatten, zodat die niet makkelijk te openen zijn. Dat hoop ik tenminste. Ik ken de situatie niet bij het AZM en kan daar dus niet over oordelen. Indien de gegevens niet versleuteld zijn en openlijk beschikbaar zijn, dan bestaat het risico dat die gegevens gestolen kunnen worden."

U noemt termen als file infector, keylogging en backdoormogelijkheden. Wat bedoelt u daarmee?

“File infector: het virus infecteert vanuit zichzelf zoveel mogelijk bestanden die eindigen op een bepaalde extensie, bijvoorbeeld exe-bestanden. Keylogging: alle toetsaanslagen die gedaan worden kunnen doorgestuurd worden naar een door de cybercrimineel te bepalen extern adres. Backdoor: zeg maar een achteringang die toegang geeft tot een netwerk.”

Uw conclusie?

“Het Sality-virus komt momenteel zeer vaak voor. Waarschijnlijk kun je ervan uitgaan dat een onwetende medewerker de bron is van de besmetting. Minder waarschijnlijk is slecht patchmanagement. Dat zou een academisch ziekenhuis op zijn minst goed op orde moeten hebben. Hetzelfde geldt voor het virusscan/security programma.”