Ziekenhuisketen met 250 vestigingen in V.S. slachtoffer van Ryuk-ransomware

Midden in de voortrazende corona-golf in de V.S. blijkt de ziekenhuisketen Universal Health Services(UHS) getroffen te zijn door een ransomware-aanval. Het betreft 250 vestigingen van dit zorgconcern. Het bedrijf maakte op 29 september 2020 melding van de problemen, die op 27 september begonnen Bijna een week later, op 3 oktober, blijkt men nog steeds bezig de oorspronkelijke staat van ICT-bedrijfsvoering te herstellen. Medewerkers kunnen medisch werk wel uitvoeren, maar de functionaliteit van het netwerk is nog niet volledig hersteld. Het herstelproces aan de servers van het datacentrum van het concern is nu voltooid. De 250 vestigingen hebben weer contact met het datacentrum, maar zijn nu bezig om hun lokale systemen veilig te laten communiceren met het datacentrum. Kortom, na een week is de impact van de aanval nog steeds merkbaar. Nergens staat enige vermelding van het betalen van losgeld aan de gijzelnemer van de systemen.

UHS

De ziekenhuisketen, met hoofdkwartier in de King of Prussia (prachtige stadsnaam trouwens) in de noordoostelijke staat Pennsylvania, slaagde er nog tijdens het opmerken van de ransomware-aanval in diverse systemen tijdig af te sluiten en netwerkverbindingen te verbreken. Zulks om verdere verspreiding tegen te gaan. Desalniettemin circuleren er berichten van medewerkers die het al bijzonder druk hadden met de corona-zorg en opeens over moesten schakelen op het

handmatig bij houden van zorgdata. Ook meldde men vertragingen met laboratoriumwerkzaamheden/- uitslagen. Medewerkers berichtten over chaotische toestanden die de patiëntenzorg betroffen, maar UHS stelt zelf dat afzonderlijke vestigingen back-ups installeerden en offline documentatiemogelijkheden gebruikten. UHZ beweert in haar persbericht van 3 oktober dat haar vestigingen de patiëntenzorg veilig en effectief verlenen. De UHS-zorg in het Verenigd Koninkrijk was niet aangedaan. Daar breidde in 2018 UHS haar activiteiten naar uit door de overname van de “Danshel”-groep.

Waarschijnlijk Ryuk-ransomwarevirus

Vanuit UHS komt alleen de melding dat er sprake is van malware op de systemen. Uit andere bronnen, o.a. door uitingen van medewerkers, blijkt er sprake van ransomware. Deze versleutelt de bestanden. Pas na betaling van losgeld laten de makers van de ransomware ontsleuteling toe. UHS maakt nergens melding van het betalen van losgeld. Wel van het herstellen van bedrijfsprocessen met hulp van gespecialiseerde bedrijven. Medewerkers zeiden bestanden gezien te hebben met de extensie “.ryk””. Dat wijst op het Ryuk-ransomware-virus. Op één van de aangedane systemen was op het beeldscherm een tekst te lezen die “Shadow of the Universe”vermeldde. Deze melding staat ook onder op het scherm bij Ryuk-virus-aantastingen. Er bestaan signalen dat UHS-systemen eerder in 2020 aangedaan waren door het Emotet- en Trickbot-virus, beide Trojan-virussen. Deze twee virussen zouden op hun beurt weer het binnenlaten van het Ryuk-vrus mogelijk gemaakt hebben.

Geen medische data gestolen?

UHS stelt in haar persverklaring van 3 oktober dat tijdens de hersteloperatie men geen indicatie heeft dat de daders toegang hadden tot data van patiënten of medewerkers, of ze kopieerden dan wel misbruikten. Geen indicatie hebben is nog geen glashard bewijs dat de data onaangetast zijn. Dat kan namelijk

later nog weleens het geval blijken te zijn.

Waarschuwing

Dit soort gebeurtenissen moet de zoveelste waarschuwing zijn om zorgsystemen bijzonder goed en voortvarend te beschermen en de processen 24/7 te monitoren. Op vele manieren kan het misgaan. In januari 2020 bleek nog dat door kwetsbare software op Citrix-servers het mogelijk was om ziekenhuissystemen in Nederland binnen te dringen. De buitenste schil werd doorbroken, verder kwamen de indringers niet. Door het realiseren van conglomeraten van ziekenhuizen, die gekoppelde hard- en software hebben, is grootschalige verspreiding van een computervirus in korte tijd mogelijk. Continue aandacht voor het versiebeheer van de software, afdoende aandacht voor cybersecurity plus segmentering van de systemen blijft continu noodzakelijk. Ook herhaald aandacht vragen voor het herkennen van phishing-mail blijft nodig. Dat is namelijk de meest voorkomende manier waarop de malware binnendringt.

W.J. Jongejan, 6 oktober 2020

Afbeelding van Mohamed Hassan via Pixabay