# Rapport mega-hack Singapore Health(juni 2018) door APT verrassend openhartig

**Op 10 januari 2019 publiceerde de onderzoekscommissie uit Singapore een 545 pagina's lang rapport over de mega-hack van SingHealth. Die afkorting staat voor Singapore Health Services Private Limited. SingHealth bracht op 20 juli 2018 naar buiten dat er persoonsgegevens van anderhalf miljoen patiënten gestolen waren plus nog 160.000 medicatiedossiers van poliklinische patiënten. Het voornaamste doel leek het medische dossier van de premier van Singapore geweest te zijn, Lee Hsien Loong. Verrassend openhartig is het rapport over de toedracht van de mega-hack.  Dat is opmerkelijk aangezien in en over de zorg men meestal niet zo open is over gecompromitteerde data.** Het betrof een zeer ingenieuze en met behoorlijke wat hulpmiddelen uitgevoerde cyberaanval die van 23 augustus 2017 tot 20 juli 2018 plaatsvond. De aanval kan beschouwd worden als een Advanced Persistent Threat(APT) die goed voorbereid geweest moet zijn. In 2017 verschafte de hacker zich toegang tot de database van SingHealth,  de SingHealth Sunrise Clinical Manager (SCM) database. Pas in de periode van 27 juni tot en met 4 juli 2018 vond de datadiefstal plaats. Tijdens de periode dat de hacker(s) actief was had men kunnen weten dat er vreemde zaken gaande waren, maar door menselijk falen vond  geen actie plaats.

## APT

Een Advanced Persistent Threat is een langdurige en doelgerichte cyberaanval waarbij een onbevoegd persoon of persnen onopgemerkt en langdurig toegang krijgt(krijgen) tot een netwerk. Het doel daarbij is om continu toegang te krijgen en gegevens te stelen. APT-aanvallen richten zich vooral op landen en organisaties. Soms worden deze aanvallen ook uitgevoerd door of namens landen, de “state linked cyber threat actors”.

## Hack

In het rapport omschrijft de onderzoekscommissie in pag. 49 t/m 96(van 425) de reconstructie van de hack. Die begon op 23 augustus 2017 met het besmetten van een werkstation, vermoedelijk door phishing email via het internet. Het aanvalsschema is te zien op pagina 53. Op dat werkstation maakte de aanvaller gebruik van een kwetsbaarheid in Microsoft’s Outlook, waarvoor al een patch bestond. En ja, het is te raden: die patch (en andere) was niet uitgevoerd. Daarna werkte de aanvaller zich langzaam van december 2017 tot juni 2018 lateraal een weg door het systeem met het binnendringen van een ander werkstation en diverse servers. Daardoor kon hij vervolgens een aantal Citrix-servers compromitteren. Met behulp van deze servers kreeg de aanvaller op 26 juni 2018 toegang tot de SCM-database. Van 27 juni tot 4 juli, dus acht dagen lang, voerde hij zoekacties uit in die database en downloadde hij bestanden.

## Ontdekt

Op 4 juli 2018 ontdekt men uiteindelijk ongebruikelijke zoekacties in de SCM-database en blokkeert men die. Daarna blijkt de aanvaller diverse pogingen gedaan te hebben o.a. met nieuwe phishing-mail om de malicieuze acties weer te hervatten. Dat lukt niet. Uiteindelijk is het op 20 juli 2018

dat de aanvallen definitief een halt wordt toegeroepen door de internettoegang tot de SingHealth-systemen volledig te blokkeren.

## MEDINT

Uiteindelijk blijken dossiers niet inhoudelijk gemuteerd te zijn. Wel maakte de aanvaller de persoonlijke gegevens van de premier Lee Hsien Loong buit en zijn poliklinische medicatiedossier. Van in totaal 159.000 mensen werd ook dat dossier buitgemaakt. Verder kopieerde de dader demografische gegevens van 1.495.364 patiënten. Het gaat dan om het NRIC nummer(National Registration Identity Card), adres, geslacht ras en geboortedatum. Te lezen op pagina 68.

De belangstelling van staten en dus “state linked cyber thread actors” voor de medische gegevens van een regeringsleider valt onder de Medical Intelligence(MEDINT), een volwassen tak van “sport” bij  inlichtingen- en veiligheidsdiensten.

## Menselijk falen

De oorzaken waardoor de aanval zo lang en zo groots uitgevoerd kon worden is gelegen in een veelvoud van menselijke en technische fouten. Te beginnen bij het onvoldoende updaten van basale programmatuur zoals email-programma, antivirus- en firewallsoftware tot het niet op de juiste manier configureren van servers de als intermediair functioneren. Daarnaast bleken er bekeerders te zijn die incompetent waren. Ze voerden benodigde patches niet uit en hadden geen goed idee wat ze beheerden. Ook ondernamen diverse personen die geacht werden onregelmatigheden te herkennen en daarop te reageren geen actie.

## Barbertje moet hangen

Je ziet helaas zoals vaak bij dit soort incidenten dat ergens in het middle-management enkele mensen ontslagen worden en de

leiding blijft zitten. Wel financieel “gestraft”  voor de gemaakte fouten. Men ontsloeg een Citrix-teamleider en een security incident response manager.

Wat wel erg goed is aan het artikel dat men de reeks van gebeurtenissen haarfijn uitgeplozen heeft en tot in detail in het rapport beschreven heeft. Dat is nogal ongebruikelijk in de ICT-wereld en zeker in de zorgsector. Het is een voorbeeld dat in Nederland absoluut navolging verdient. Het onder het vloerkleed vegen levert niet een les op die uiteindelijk toch geleerd moet worden.

Daarnaast kan heel simpel geconcludeerd worden dat het koppelen van zorgdatabases aan het internet geen verstandige keuze is.

W.J. Jongejan, 22 januari 2019