Extra aandacht voor “refurbished” medische hardware nodig bij ontdekking kwetsbaarheden

Elektronische medische apparatuur is al enige tijd een prooi voor hackers. Ik schreef er op deze website al meerdere keren over(A, B, C). Op de website van het online magazine The Register stond op 13 juni 2019 een artikel waarin men duidelijk maakte dat een elektronisch werkstation dat infuuspompen aanstuurt en data naar een centrale computer verstuurt twee flinke kwetsbaarheden blijkt te hebben. Daardoor kunnen kwaadwilligen de aansturing overnemen en de patiënt schade berokkenen dan wel daarmee dreigen. Het gaat om het ALARIS Gateway Workstation van de firma Becton Dickinson, beter bekend onder de afkorting BD. Eén van de ontdekte kwetsbaarheden betreft de firmware van het apparaat die door een aanvaller op afstand vervangen kan worden door een eigen bedachte variant. De andere kwetsbaarheid zit in de web-based interface van het werkstation. Die aansluiting van het werkstation op een lokaal netwerk maakt de apparatuur kwetsbaar voor aanvallen. Zeker als het lokale netwerk nog ergens in de organisatie op het internet is aangesloten. Zorginstellingen zullen hun cybersecurity moeten aanscherpen en nieuwe firmware moeten installeren. Inmiddels bestaat er ook een levendige officiële handel in tweede hands medische apparatuur. Door “refurbishing” maakt men die dan opnieuw klaar gemaakt voor de markt. Ook in die sector dient men zeer alert te zijn op het installeren van zeer recente firmware.

Alaris Gateway Workstation

Dit werkstation maakt het mogelijk om data van infuuspompen te integreren in het centrale elektronische informatiesysteem van het ziekenhuis. Dat kan bekabeld maar ook draadloos via een wifi-netwerk. BD maakt in haar reclame-uitingen op het internet kenbaar dat dit systeem de artsen en verpleegkundigen de totale controle over de aangesloten apparatuur geeft. Helaas kunnen hackers dat met de gemelde kwetsbaarheden in de software ook. Het is trouwens maar helemaal de vraag of dergelijke apparatuur wel 24/7 aan lokale netwerken of het internet gekoppeld dient te zijn.

CVE

Sinds 1999 worden alle kwetsbaarheden in soft- en hardware in het kader van cybersecurity bijgehouden op een lijst met de naam Common Vulnerabilities and Exposure. Die krijgt wereldwijde input. De databank wordt onderhouden door het bedrijf MITRE Corporation en de nationale divisie voor informatiebeveiliging van het Amerikaanse Departement van Binnenlandse Veiligheid financiert die. Voor publicatie plaats vindt gaan de meldingen naar ICS-CERT. Deze organisatie maakt ook apart melding van incidenten. Kwetsbaarheden worden aangeduid met de afkorting van die naam: CVE, het jaartal van ontdekking en een volgnummer.

CVE-2019-10959

De eerste van de twee gerapporteerde kwetsbaarheden t.a.v. het Alaris werkstation is er één die het mogelijk maakt dat een aanvaller de firmware van het apparaat vervangt door eigen maaksel van de hacker. Met die verandering kan de aanvaller de dosering van de aangesloten infuuspompen manipuleren. Deze kwetsbaarheid is zo ernstig dat het een ernst-score van tien op een schaal van tien krijgt.

CVE-2019-110962

Deze kwetsbaarheid krijgt een score van 7,3 op de schaal van tien en is gelokaliseerd in de web-based interface van het werkstation. De aanvaller kan als hij het IP-adres van het werkstation kan herleiden toegang krijgen tot event-logfiles en de configuratie van het werkstation om die dan naar zijn hand te zetten.

Remedie

De remedie voor deze kwetsbaarheden is het installeren van de allernieuwste firmware die Becton Dickinson voor de Alaris werkstations maakte. Het gaat dan om de versies 1.3.2 en 1.6.1. Daarmee zou het probleem opgelost zijn. Tot die tijd adviseren experts het minimaliseren van het aantal netwerkverbindingen voor alle medische apparaten en systemen. Daarnaast ook het isoleren van de apparaten achter firewalls, het ontwikkelen van adequate en diepgaande verdedigings-strategieën(bijv. compartimentering) en het opdoeken van niet noodzakelijke protocollen, accounts en diensten.

Gebruikte medische apparatuur

De laatste jaren is er een levendige handel ontstaan in medische elektronische apparatuur, deels afkomstig van bedrijfsbeëindigingen, deels van zorgaanbieders die hun spullen vervangen door modernere versies. De apparaten reinigt en reviseert men, maar verreweg het allerbelangrijkste is dat deze hardware van adequate en de meest verse soft-/firmware wordt voorzien. Dat lijkt een absolute vereiste, maar daar gaat wel eens wat mee mis. Zowel nationaal als internationaal zijn bedrijven actief. Zo is er in ons land bijv. het bedrijf Mediproma actief en doet zelfs Philips aan het na revisie opnieuw op de markt brengen van scan- en Röntgenapparatuur. Ook internationaal zijn er flink wat bedrijven actief zoals Master Medical Equipment(MMEMed) en DotMed.

Oude data nog aanwezig

Vrij recent, in mei 2019, vond in Amsterdam de Hack In The Box cybersecurity conferentie plaats. HITB is een organisatie die zich bezig houdt met cyberveiligheid. Tijdens de conferentie was er ook een “Medical Security Village”. Dat was een plaats waar infosecurity onderzoekers in contact konden komen met verkopers van elektronische medische apparaten. Niet alleen om van elkaar te leren , maar ook om apparatuur te testen. Zo was ook Philips daar aanwezig met mensen van hun security-team. In het kader van die conferentie vond een workshop plaats waarbij men een gekocht gerenoveerd apparaat op de “pijnbank” legde. Het ging om een monitor voor radiologiebeelden. Na korte tijd bleek te achterhalen uit welk ziekenhuis het apparaat kwam en dat er nog patiëntgegevens op stonden. Blijkbaar was de revisie op software-/firmware vlak niet rigoureus genoeg geweest. De ethische hackers lichtten meteen het ziekenhuis en de leverancier in waar het apparaat vandaan kwam.

Moraal van het verhaal

De les die uit het bovenstaande getrokken kan worden dat niet alleen in zorginstellingen het schort aan voldoende besef van cyberveiligheid. Ook voor revisie- (“refurbishing”)bedrijven ligt blijkbaar de lat niet altijd hoog genoeg. Waken over cyberveiligheid moet niet een stiefkind zijn binnen organisaties en bedrijven maar een continu proces. Daarbij dient men ogen en oren voor en achter in het hoofd te hebben.

W.J. Jongejan, 19 juni 2019

De op de foto getoonde elektronische infuuspomp lijkt geen Alaris Gateway Workstation van Becton Dickinson(BD) te zijn.