Beklemmende tango verkoper en koper zorg-ICT-systemen oorzaak onveiligheid

De uitspraak “It takes two to tango” heeft in de wereld van de zorg-ICT een bijzondere betekenis. In de eerste plaats is er in toenemende mate sprake van een vendor lock-in. Dat is een situatie waarbij de zorginstelling niet in staat is om van leverancier te veranderen zonder substantiële omschakelingskosten of ongemak. Dat komt door òf een beperkt aantal leveranciers van ICT-systemen òf door een aantal vaste koppelingen tussen systemen. Daardoor is overstappen op andere leveranciers praktisch onmogelijk. Daarnaast kan het zo zijn dat volkomen verschillende belangen van zowel de verkopende partij als de kopende partij een beklemmende situatie oplevert. In een zeer aardig artikel op de website The Register op 19 juni 2018 laat de schrijver ervan Ophir Zilbiger aan het woord. Hij was spreker op de Israël Cyber Week die van 17 tot en met 21 juni 2018 in Tel Aviv gehouden werd. Zilbiger staat aan het hoofd van BDO Cybersecurity Center Israel Consultancy. Hij legde haarfijn uit hoe het komt dat zorg-ICT-systemen kwetsbaar zijn voor malware en andere virussen. Dat komt volgens hem door het enorme verschil in focus tussen koper en verkoper van die systemen, terwijl die twee elkaar toch hard nodig hebben.

Verkoper

De verkopende partij, zo stelt Zilbiger, ontwikkelt nieuwe systemen die moeten voldoen aan een groot aantal medische eisen en aan vaak strikte regelgeving, bijv. van de Food and Drug Adminstration(FDA) in de V.S. Om daaraan te voldoen is er vaak sprake van een lange ontwikkelingstijd. Dat zorgt voor een probleem, omdat als medische apparatuur met ICT-systemen aan boord na een lange ontwikkelingsperiode verkocht wordt, de verkoper weer gefocust is op de ontwikkeling van een geheel nieuwe generatie apparatuur. Hij is daardoor niet erg gespitst op het upgraden van verkochte apparatuur en ziet niet goed toe op het verbeteren van verkochte, bestaande systemen. Uit het oogpunt van cybersecurity is dat een heel slechte zaak.

Koper

Zilbiger merkt terecht op dat ziekenhuizen over het algemeen grote moeite hebben om een goede balans te vinden tussen de uitgaven voor medische apparatuur en de eisen die cybersecurity aan de instellingen stellen. En dat met vaak teruglopende of beperkte budgetten. Bovendien zijn zorginstellingen vaak met de handen gebonden, omdat ze vaak niet eigenstandig modificaties aan soft- en hardware mogen en kunnen uitvoeren. Dat is dan op basis van de bestaande contracten met de leverancier. Daardoor ontstaat de situatie dat besturingssystemen niet geüpdatet worden en daardoor malware- en andere virusaanvallen mogelijk zijn.

Veranderingen

In het handelen van zowel de verkopende als kopende partij van medische ICT-systemen dienen daarom een aantal veranderingen plaats te vinden. De verkoper zal meer dan voorheen erop dienen te letten dat verkochte apparatuur qua software, vooral ten aanzien van besturingssystemen, up-to-date zijn op het moment van verkoop. En de systemen door de koper eenvoudig, liefst automatisch te updaten zijn.

Ook dient de verkopende partij meer dan voorheen een alerte

afdeling software-support te hebben waardoor er ook een duidelijk focus is op het onderhoud van verkochte systemen. De koper zal meer dan voorheen alert moeten zijn op het al dan niet adequaat geüpdatet zijn van systemen, zowel operationeel als qua cybersecurity. In de contracten die afgesloten worden dient de koper meer dan voorheen passende en blijvende ondersteuning door de verkopend partij te eisen en vast te leggen.

Tango

De tango is een dans waarin de melancholie, vaak het lijden, verbeeld wordt. Uit het voorgaande moge duidelijk zijn dat verkoper en koper van zorg-ICT-systemen elkaar vaak gevangen houden in een relatie die tot lijden leidt.

W.J. Jongejan, 22 juni 2018