AZ Vesalius – Veilige toegang tot patiëntengegevens

De nood naar digitale beveiliging bij ziekenhuizen en verzorgingscentra wordt steeds groter. Het AZ Vesalius is een zorgcentrum in Tongeren, met jaarlijks meer dan tienduizend gewone opnames en zestienduizend spoedopnames. Het AZ Vesalius koos onder andere voor F-Secure omdat het wil vermijden dat cryptolockers de dagelijkse werking gaat beïnvloeden of dat medische gegevens worden gelekt. “Alles draait rond toegang tot de juiste patiëntengegevens. Daar hangt de kwaliteit van onze zorgen af,” zegt Wouter Soogen van het AZ Vesalius.

“We werken met wel 150 servers, die allemaal aan elkaar gekoppeld zijn. Intussen zijn bijvoorbeeld ook sommige spuitpompen en monitors aan het netwerk gekoppeld. Die kunnen dan rechtstreeks gegevens doorsturen naar het medisch dossier dat dan overal geconsulteerd kan worden.”, weet Soogen.

Cryptolockers en gelekte medische dossiers

Het AZ had in 2015 en 2016 wel drie keer te lijden onder een cryptolocker, gelukkig zonder veel erg. Eerst werd een paar pc’s geëncrypteerd. Bij een latere poging raakten de fraudeurs echter tot op het netwerk. Tijd om in te grijpen dus. “We merken dat er steeds meer aanvallen komen. Tot enkele jaren geleden kregen we af en toe een klein virusje over de vloer. Maar het gaat in stijgende lijn. Een partner van ons kreeg af te rekenen met gelekte medische dossiers. Dat wil je als ziekenhuis niet meemaken.”

Als extra motivatie: de Belgische minister van gezondheidszorg werkt aan een plan om medische dossiers vlot uitwisselbaar te maken. Dat op een veilige manier doen, wordt een belangrijke uitdaging. Er hangt ook een financieel voordeel aan vast. De financiering van de ziekenhuizen zal voor een deel gaan afhangen van deze data uitwisseling en dit willen we dan op een veilige manier zien gebeuren. “Vergeet verder ook niet dat GDPR eraan komt. Zeker in de gezondheidssector staat dit als uitdaging met stip bovenaan het lijstje.”, vult Soogen aan.

Penetration test

Na de verschillende incidenten koos het AZ Vesalius ervoor om een *penetration test* te laten uitvoeren. Een hacker trachtte op verschillende manieren om het ziekenhuis digitaal te infiltreren, zowel extern als intern. Daar kwamen een aantal interessante resultaten uit. “Elke nieuwe toepassing die op het netwerk wordt geënt zorgt voor nieuwe risico’s. Dat is het nadeel van het feit dat alles overal raadpleegbaar moet zijn.” Het securityrapport was echt een eyeopener en leidde ertoe dat het AZ Vesalius op zoek moest naar een stabiele partner voor databeveiliging.

F-Secure als beter alternatief voor nextgen

Het ziekenhuis richtte een zogenaamde *proof of concept* (POC) in om de beste oplossing voor hun uitdagingen te vinden. “We hebben eerst een aantal next-gen producten doorgelicht. Die nieuwe generatieproducten werken niet meer op basis van *hashes*, maar meer heuristisch. Ze beveiligen op basis van het gedrag van het programma. De resultaten vielen wel mee, maar we merkten wel dat ze nog niet helemaal klaar waren om 100% beveiliging te bieden. De nextgen’s raadden zelf aan om hun oplossingen samen met een traditioneel anti-viruspakket te implementeren. Als we een nextgen oplossing met een meer traditioneel end-point-securityproduct moeten gaan combineren, dan zaten we ver boven ons voorziene budget.”, concludeerde Soogen.

Een ander probleem van nextgen-toepassingen is dat de virussen ook echt actief moeten zijn vooraleer ze kunnen worden opgespoord. Ook dit was een minpunt voor het AZ Vesalius. Ze zochten een oplossing die proactief op zoek gaat naar bedreigingen.

Na de sales, de praktijk

Tijd om verder te kijken dus. De POC werd verdergezet. In een labo-omgeving werden honderd virussamples op de oplossing van F-Secure en die van twee concurrerende oplossingen losgelaten. “F-Secure sprong hier echt tussenuit, ook al omdat we toch ook op zoek waren naar een oplossingen met de voordelen van *nextgen*: F-Secure scoorde goed op *hashes*, maar blokkeerde ook op basis van het gedrag.” Mooie extra was dat DeepGuard van F-Secure de vergrendelde toepassingen ook ontgrendelde.

> *“We leerden F-Secure beter kennen tijdens een eerste salesgesprek. Salesmensen verkopen hun product natuurlijk altijd vlot, maar het was de praktijktest die de doorslag heeft gegeven.”*

Na de POC werd een analyse gemaakt van de verschillende oplossingen. Hier werd rekening gehouden met verschillende elementen: de resultaten van de POC, maar ook de totale kostprijs voor heel het project. “F-Secure was prijs/security-gewijs gewoon de beste keuze. Ze zijn met glans geslaagd.”

Verrassend vlotte installatie

Na de bestelling van het product kreeg het AZ Vesalius de licenties. Een technicus van F-Secure kwam naar Tongeren om daar de management-server op te zetten. “Eerst en vooral moest de oude antivirussoftware verwijderd worden, vooraleer het product van F-Secure kon worden geïnstalleerd. We hadden met dit proces wat problemen verwacht, maar alles is eigenlijk verrassend vlot verlopen.”

Wouter Soogen is tot op heden een erg tevreden F-Secure gebruiker: “We krijgen e-mailalerts bij virusaanvallen. De rapportering loopt erg vlot en het gebruik wijst zichzelf uit. Het enige puntje van commentaar is dat we graag een wat uitgebreidere *application and device control* module hadden willen hebben. Het siert F-Secure dan wel weer dat deze uitbreiding nu al op de planning staat.”