”Security is altijd teveel, tot de dag dat het niet genoeg is”

Franciscus Gasthuis & Vlietland integreert IT- en security-infrastructuur met Conscia NOC en SOC-dienstverling

Franciscus Gasthuis & Vlietland biedt met twee ziekenhuizen in Rotterdam en Schiedam en drie buitenlocaties (poliklinieken) zorg zo dicht mogelijk aan bij de woonomgeving van mensen.

De 4700 medewerkers en 300 artsen richten zich op topzorg met een sterk menselijk karakter. Om hun werk in goede banen te leiden, draait er een IT-netwerk met zo’n 10.000 aangesloten endpoints zoals computers, servers, medische modaliteiten, mobile devices etc. Deze worden gebruikt door zowel de directe zorgverlenende medewerkers, als de collega’s in ondersteunende functies. Het beheer van dit netwerk buiten kantoortijden was al geruime tijd ondergebracht bij Conscia, en hier is nu de security-ondersteuning bijgekomen.

Peter de Boer
Manager ICMT
Franciscus Gasthuis & Vlietland

Jos Toet
Information Security Officer
Franciscus Gasthuis & Vlietland

Digitale zorg vraagt om aanscherpen security

De zorg is aan het veranderen. Deze vindt niet langer alleen in het ziekenhuis plaats, maar is steeds meer locatie-onafhankelijk.

Door de inzet van digitale middelen, kan zorg steeds meer op afstand plaatsvinden. Dit heeft gevolgen voor de security-strategie van het ziekenhuis en voor de inrichting van de security-organisatie; een IT-onderdeel dat al onder druk staat door de toenemende dreiging van aanvallen en misbruik van kwetsbaarheden. Franciscus Gasthuis & Vlietland wilde de security-maatregelen aanscherpen en had de wens om dit niet langer geheel in eigen beheer te doen. Uit een eerste marktverkenning voor een Security Operations Center (SOC) dienst-verlening, bleek dat veel aanbieders een oplossing bieden met een hoge mate van maatwerk en een bijpassend hoog kostenplaatje. Franciscus Gasthuis & Vlietland implementeerde samen met Conscia een passende, doeltreffende oplossing die tegelijkertijd kosteneffectief is.

Integrale security-benadering

Als onderdeel van de integrale security-aanpak zijn de diverse puntoplossingen waar het ziekenhuis gebruik van maakte, vervangen door een Cisco Secure CyberSecurity-platform waarin de samenwerking tussen de producten betere security en bovenal meer inzicht levert tegen een lagere beheerlast.

Na deze eerste stap heeft Franciscus Gasthuis & Vlietland eind 2021 besloten de aspecten monitoring en detectie grotendeels onder te brengen bij het SOC van Conscia. Dit in nauwe samenwerking met het IT Security Team van Franciscus, dat wordt gezien als de interne 'digitale brandweer', die participeert op het vlak van Identify, Protect, Detect, Respond en Recover.

Door eerst alle losse puntoplossingen te vervangen door een suite van security-tools en -maatregelen die onderling correleren, kon het SOC een stuk sneller en goedkoper worden ingeschakeld, omdat er nauwelijks maatwerk nodig was.

Peter de Boer, Manager ICMT bij Franciscus Gasthuis & Vlietland: "Waar we voorheen een traditionele beheerorganisatie waren, krijgt onze IT-afdeling steeds meer een functionele ondersteuningsrol richting de zorg. Hierdoor worden steeds meer taken uitbesteed, en dat wilden we nu ook met een deel van het security-beheer doen. In de zorg spelen andere belangen dan in andere sectoren, en hebben we te maken met andere budgetten. Ook is het steeds lastiger om de juiste security experts te vinden en hun kennis up-to date te houden. Hierdoor moesten we op zoek naar een partij die dat begrijpt en mee zoekt naar een passende oplossing. Bij de keuze voor Conscia speelt ook vertrouwen een belangrijke rol. Door de goede, langdurige samenwerking met hen konden we de keuze weloverwogen en overtuigd nemen."

Daarnaast speelde mee dat de zorgorganisatie al gebruik maakt van Conscia's Network Operations Center (NOC) dat gekoppeld kan worden aan het SOC. Op die manier kunnen de experts bij Conscia snel ingrijpen bij incidenten en de gevolgen voor het netwerk overzien en minimaliseren. De kennis van de NOC- en SOC-specialisten vormen een waardevolle aanvulling op het IT-team van de zorgorganisatie.

"Waar we voorheen een traditionele beheerorganisatie waren, krijgt onze IT-afdeling steeds meer een functionele ondersteuningsrol richting de zorg."

De Boer: "Naast de traditionele IT-apparatuur hebben we ook steeds meer te maken met medische apparatuur, zoals bewakingsmonitoren, echografie, ECG's etc, die aan het netwerk gekoppeld worden. De samenkomst van Medische Technologie (MT), Informatie Technologie (IT) en Operationele Technologie (OT), zoals gebouwenbeheersysteem, het medisch oproepsysteem en de brandmeldinstallatie, zorgt voor extra security-uitdagingen. Daarom is de koppeling van een NOC en een SOC een mooie oplossing. We hebben op alle vlakken inzicht nodig in het dataverkeer. Preventie is van belang, maar alléén het dichttimmeren van een organisatie heeft geen zin, want er gebeurt ook genoeg binnen de muren van je infrastructuur en je hebt daarbij onder meer te maken met gedrag van medewerkers. We moeten die datastroom onder controle hebben, en daar zijn we nu veel beter toe in staat."

Managed Detect & Response

Preventie van cybercrime in de vorm van firewalls en trainingen is belangrijk maar niet voldoende. Detectie is ook nodig om te weten wanneer er toch een incident plaatsvindt. En dan is het zaak snel in te grijpen. Door de combinatie van NOC en SOC is dit goed mogelijk. Bovendien is dit, door het als managed service af te nemen, snel uit te rollen. Security wordt op die manier overzichtelijk, snel en kostenefficiënt.

Jos Toet, Information Security Officer bij Franciscus Gasthuis & Vlietland: “Security is altijd te veel, tot de dag dat het niet genoeg is. Vaak is het idee dat security achter de schermen plaatsvindt en niet bijdraagt aan de patiëntenzorg, maar het draagt wel degelijk bij aan de continuïteit van de zorg en de beschikbaarheid, integriteit en vertrouwelijkheid van alle gegevens die gewaarborgd moet blijven. Daarnaast is goede security grotendeels afhankelijk van het gedrag van mensen. We kunnen alles technisch dichttimmeren, maar als een medewerker zijn computer onbeheerd open laat staan, heeft de beveiliging toch gefaald.

> “Security is altijd te veel, tot de dag dat het niet genoeg is. Vaak is het idee dat security achter de schermen plaatsvindt en niet bijdraagt aan de patiëntenzorg, maar het draagt wel degelijk bij aan de continuïteit van de zorg en de beschikbaarheid, integriteit en vertrouwelijkheid van alle gegevens die gewaarborgd moet blijven.”

Toet: “Security hoeft de patiëntenzorg helemaal niet in de weg te staan, juist niet. We faciliteren nu veel meer wat wel kan en mag, in plaats van dat we allemaal zaken verbieden. We willen iedereen op die manier intrinsiek motiveren om zorgvuldig te handelen en bewust te worden van de risico’s. En dat werkt; we merken nu al meer betrokkenheid en bewustwording bij collega’s uit allerlei geledingen. Door de focus op security zie je dat kennis erover groeit. Bij de mensen in het IT-team tot aan de mensen aan het bed. En dat is mooi om te zien.”

Overview

IT-security onderbrengen in SOC

De verzameling security-oplossingen bij het Franciscus Gasthuis & Vlietland vormden geen eenheid, en boden weinig toekomstperspectief voor beheer en beveiliging van het ziekenhuis in een digitaal tijdperk. Dit zorgde voor de noodzaak om samen met Conscia bepaalde taken rond beheer en security uit te besteden. Door in te zetten op een platform en beheer en security te beleggen via een managed service en SOC, legt het ziekenhuis een goede basis voor een veilige digitale toekomst.

Oplossing

Conscia Managed Detect & Response SOC-services
Cisco Secure CyberSecurity-platform

Resultaten

- Verhoogde veiligheid van het ziekenhuis, toekomstbestendig, minder beheer, hogere betrouwbaarheid
- Snelle ingreep door koppeling NOC en SOC
- Kostenefficiënt door combinatie Conscia-diensten en Cisco-platform
- Goede (of betere) samenwerking tussen Franciscus en Conscia
- Security-bewustwording in de organisatie

Wil je ook eens keer praten over jouw IT- en security-infrastructuur?

Neem contact op