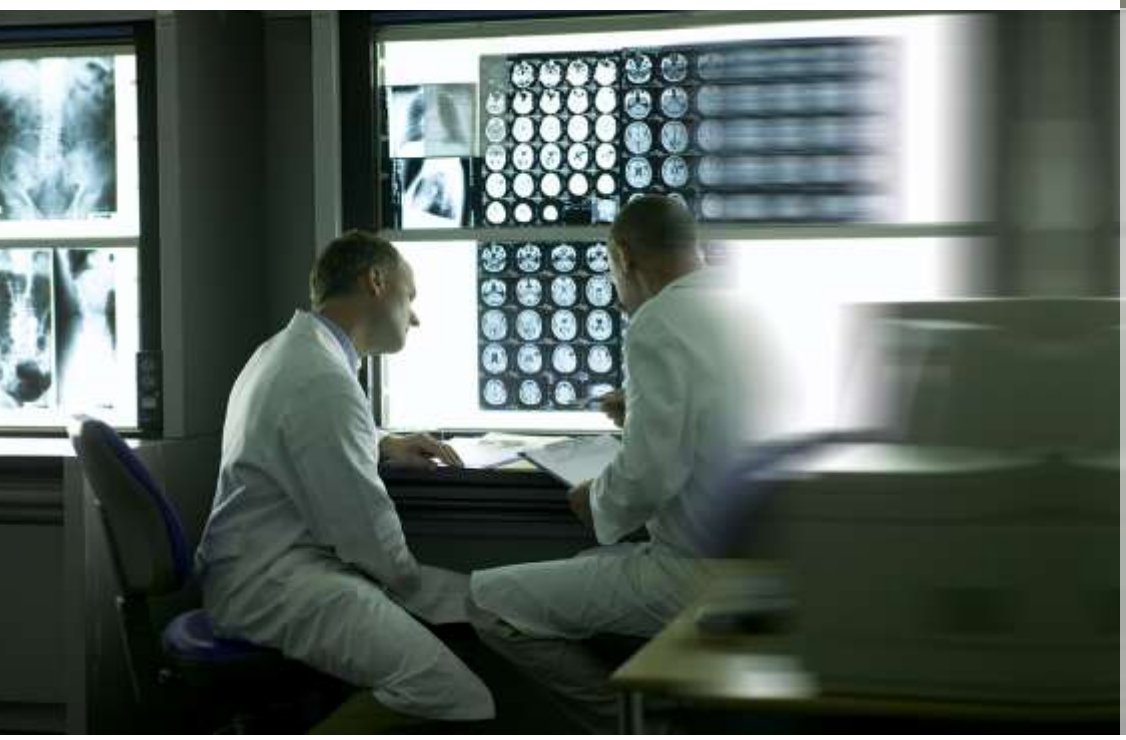

GGD Brabant Zuidoost

Dankzij Fortinet hebben we geen omkijken meer naar de IT-beveiliging en deze is meer up-to-date dan ooit. Het grootste voordeel is dat alle producten volledig samenwerken en eenvoudig beheerd kunnen worden vanuit één console.

– Jurgen Mol, manager systeembeheer van GGD Brabant Zuidoost

GGD Brabant Zuidoost houdt netwerk veilig en gezond met Fortinet

De GGD Brabant-Zuidoost helpt 21 gemeenten in de regio om haar inwoners gezonder te maken én te houden. De GGD adviseert gemeenten over hun gezondheidsbeleid en voeren dit deels uit. Maar ze werken ook veel samen met de 'reguliere' zorg, zoals huisartsen en ziekenhuizen. De zorgverleners staan dag en nacht klaar om de gezondheid van de inwoners te beschermen.

De ICT-afdeling ondersteunt dit streven met informatiesystemen die net zo alert, beschikbaar en operationeel zijn als de medewerkers. Nu én in de toekomst. Malware mag deze taak niet verlammen en daarom wil men de risico's spreiden. De ICT-afdeling zocht niet één allesomvattende oplossing voor ICT-beveiliging, maar een familie aan gespecialiseerde, samenwerkende producten. Die vond men in het portfolio van Fortinet.

Alle gemeenten in Nederland hebben de taak om de gezondheid van hun inwoners te beschermen en te verbeteren. Dat doet men enerzijds met preventieve acties, om te voorkomen dat mensen ziek worden en anderzijds met snelle interventies, bijvoorbeeld de ambulancezorg. De GGD Brabant Zuidoost voert deze taak voor 21 gemeenten in de regio uit.

De zorgverlening staat in Nederland door de 'dubbele vergrijzing' enorm onder druk. Meer mensen leven langer en dat maakt betaalbaarheid van de zorg uitdagend. Zorg moet efficiënter geleverd worden, zonder concessies te hoeven doen aan de toegankelijkheid of kwaliteit. De zorgsector is daardoor continu in ontwikkeling. Dat maakt het lastig om te

Details

Naam bedrijf: GGD Brabant Zuidoost

Industrie: Healthcare

Locatie: Eindhoven, Netherlands

Zakelijke voordelen

- Met de Fortinet-appliances kan de GGD nieuwe beveiligingsfuncties toevoegen en andere beveiligingsapparaten samenvoegen, zoals IPS, antimalware en antiphishing, flexibele webfiltering en inzicht en rapportage
- De FortiGate 500D beschikt over de nieuwste FortiASIC NP6-processors die een doorvoersnelheid van 16 Gbps levert
- Dankzij de op maat gemaakte rapporten van FortiAnalyzer worden gegevens gefilterd en beoordelen, met inbegrip van traffic, events, virussen, aanvallen, web-inhoud en e-mail
- De Fortinet-oplossingen ondersteunen het voldoen aan de Wet Meldplicht Datalekken

Voorspellen welke diensten, en bijbehorende netwerkcapaciteit, de ICT-afdeling in de nabije toekomst moet bieden. Marco van de Paal en Jurgen Mol, managers systeembeheer van GGD Brabant Zuidoost, vertellen hoe Fortinet de GGD Brabant Zuidoost hielp om de beschikbaarheid van de ICT-systemen voor de toekomst te waarborgen.

De situatie

"In 2015 was onze firewall, die het netwerkverkeer beschermt tegen malware, virussen en hackers, nodig aan vervanging toe," zegt Van de Paal. "De apparatuur voldeed niet meer aan de eisen van deze onze organisatie, noch aan de richtlijnen voor een veilige omgang met informatie in de gezondheidszorg (NEN 7510). Ook konden we met de oude firewall de Wet Meldplicht Datalekken binnen de Wet bescherming persoonsgegevens niet naleven. Daarmee begon de zoektocht naar een nieuwe oplossing voor IT-beveiliging, die voldoende flexibiliteit, schaalbaarheid en capaciteit biedt om onze systemen en medewerkers ook in de toekomst te beschermen."

De onvoorspelbaarheid is dat de GGD in 2015 de ambulancezorg overnam van de Veiligheidsregio Brabant-Zuidoost (VRBZO). "De Regionale Ambulance Voorziening kwam onder onze hoede en dat betekent dat we alle applicaties van deze dienst moeten integreren met ons netwerk," zegt Mol. "Dat stelt natuurlijk ook meteen zwaardere eisen aan de beschikbaarheid, want deze is voor de ambulancezorg niet alleen bedrijfskritisch, maar echt van levensbelang. Ons netwerk dient dus meer dan ooit tevoren 24x7 beschikbaar te zijn."

De GGD krijgt niet alleen te maken met meer medewerkers die buiten kantoortijden werken, maar ook buiten de kantoormuren. "We werken in een cloudomgeving van Citrix, maar het netwerk binnen het pand is een LAN," zegt Van de Paal. "Dat is nog relatief eenvoudig te beveiligen. Er zijn echter steeds meer mensen die toegang op afstand nodig hebben. Dat geldt vanzelfsprekend voor de medewerkers van de ambulancezorg. We hebben ook circa 150 ambulante medewerkers die bijvoorbeeld naar scholen en instellingen gaan. Maar eigenlijk is elke medewerker is een potentiële thuiswerker. We moeten dus voorbereid zijn op het feit dat er ruim 500 mensen op afstand toegang willen tot ons netwerk."

Naast de medewerkers vragen ook burgers om meer online toegang en selfservice, weet Mol. "Op dit moment kunnen burgers alleen reizigersvaccinaties regelen via website, maar er zijn zeker plannen om dit in de toekomst uit te breiden. Op termijn kan men via de website bijvoorbeeld afspraken maken voor een consult, een digitaal spreekuur volgen of andere zorg regelen. Dat brengt een grote toename in de vraag naar netwerkcapaciteit en -beveiliging met zich mee."

De oplossing

De ICT-afdeling van GGD Brabant Zuidoost nodigde verschillende leveranciers uit om voorstellen en presentaties te geven over hun oplossingen voor IT-beveiliging. "We hebben ook zelf ons huiswerk gedaan," aldus Van de Paal. "We onderzochten bijvoorbeeld welke oplossingen er gebruikt worden bij andere GGD-instellingen. We lazen de testrapporten van NSS Labs en bekeken de waarderingen van grote internationale onderzoeksbureaus. Natuurlijk beschikken we zelf over een brede expertise op het gebied van IT, maar zijn geen beveiligingsspecialisten. Daarom wonnen we ook het advies in van ICT-dienstverlener 4IP."

"In onze optiek is het beter om de firewall en virusscanning te scheiden. Dat biedt een betere spreiding van de risico's. We wilden echter wel de voordelen van een centrale beheerconsole, zoals bij een UTM, behouden. Daarom zochten we een reeks producten met gespecialiseerde beveiligingsfuncties die uitstekend samenwerken en gezamenlijk beheerd kunnen worden."

Uit de onderzoeken en gesprekken met 4IP bleek al snel dat Fortinet de beste oplossingen had voor GGD Brabant Zuidoost. Mol: "Fortinet heeft een aantal beveiligingsoplossingen die goed samenwerken en centraal beheerd kunnen worden. Via 4IP kwamen we in contact met het Nederlandse team van Fortinet en liepen met hen het wensen- en eisenlijstjes door. Zij gaven ons veel waardevolle adviezen voor onze situatie."

Uit deze gesprekken kwam ook de geruststelling dat Fortinet een oplossing bood waar de GGD nog jaren mee vooruit kan. "Bovendien wilden een productlijn met de beste prijs-kwaliteit verhouding," aldus Van de Paal. "Bij Fortinet vonden we dit. Het bedrijf levert oplossingen die klaar zijn voor de toekomst, want men is heel innovatief en constant bezig met nieuwe ontwikkelingen. Dat blijkt ook uit de testen van NSS Labs en het feit dat Fortinet uitstekend scoort in het magische kwadrant van een internationaal onderzoeksbureau. De functionaliteit en capaciteit is schaalbaar en dat is belangrijk, want we kunnen nu nog niet zeggen hoeveel data er in de toekomst over het netwerk gaat. Wat we nu hebben kan over twee jaar alweer te weinig zijn."

FortiGate

De GGD Brabant Zuidoost installeerde twee FortiGate 500D-appliances in het eigen datacenter. Deze zijn redundant uitgevoerd: in het geval van storingen zal de ene firewall de andere vervangen. De FortiGate is een zogenoemde Next-Generation Firewall (NGFW) die het netwerkverkeer op een dieper niveau kan inspecteren. "Met deze appliances kunnen we niet alleen nieuwe beveiligingsfuncties toevoegen, maar ook de andere beveiligingsapparaten uit het portfolio van Fortinet samenvoegen," zegt Mol. "Dat komt doordat de appliances beschikken over de functies van het FortiOS platform voor netwerkbeveiliging, zoals IPS, antimalware en antiphishing, flexibele webfiltering en inzicht en rapportage."

NGFWs voorzien in meer én efficiëntere beveiliging dan traditionele firewalls. Van de Paal: "Vanwege het toenemende aantal mobiele en flexwerkers is het belangrijk dat we al op de toegangspoort geavanceerde bedreigingen af kunnen weren. Bovendien zijn we nu beschermd zijn tegen malware op de dag dat deze ontstaat."

De FortiGate 500D beschikt bovendien over de nieuwste FortiASIC NP6-processors, die zorgen voor snelle firewallprestatie en beter VPN-beheer. "Dankzij deze processors kunnen we het netwerkverkeer beter vormgeven en voorrang geven aan prioriteiten," aldus Mol. "De FortiGate-500D, levert bovendien een doorvoersnelheid van 16 Gbps en is uitermate schaalbaar. De oplossing kan wat betreft maximale belasting zoveel aan dat we hier zeker niet tegen beperkingen gaan aanlopen. Voor de toekomst zitten we dus nog wel even goed."

FortiAnalyzer
Voor de rapportage over het netwerkverkeer gebruikt de GGD FortiAnalyzer, vervolgt Mol. "Deze verzamelt, analyseert en rapporteert de gegevens uit de producten van Fortinet. Dat geeft waardevolle overzichten van wat er speelt en zodoende weten we precies wat we in de gaten moeten houden."

Dankzij de op maat gemaakte rapporten van FortiAnalyzer kan de GGD gegevens filteren en beoordelen, met inbegrip van traffic, events, virussen, aanvallen, web-inhoud en e-mail. "FortiAnalyzer biedt bovendien geavanceerde beheersfuncties om bestanden in quarantaine te plaatsen, incidenten te correleren, kwetsbaarheden te beoordelen, het verkeer te analyseren, en nog veel meer," vertelt Van de Paal. "Dat gaat allemaal via een gebruiksvriendelijk en overzichtelijk dashboard, met duidelijke notificaties en meldingen."

FortiClient
Voor de beveiliging van de desktops, laptops, tablets en smartphones van de eindgebruikers, koos GGD Brabant Zuidoost voor FortiClient Element Management System (EMS). "Deze verbindt de apparaten van vaste en mobiele werknemers met de FortiGate firewall," legt Mol uit. "Dit maakt het eenvoudiger om endpoints uit te rollen vanuit de centrale beheeromgeving. We kunnen hiermee allerlei beveiligingsmaatregelen installeren op de apparaten, zoals antivirus, VPN, application firewalls, kwetsbaarheidsscan en internetbeveiliging."

FortiMail
Het e-mailverkeer van en naar de GGD wordt beveiligd met FortiMail VM-01. Dit is een compleet platform voor het beveiligen van zowel binnenkomende als uitgaande e-mail. FortiMail beschermt tegen dreigingen en dataverlies met functies zoals antispam, antiphishing, antimalware, data leakage prevention, identity based encryption (IBE), message archiving en antiblacklisting. "Met FortiMail blokkeren we spam en malware voordat het de gebruikers bereikt," zegt Van de Paal. Dat verkleint het risico tot het verlies van vertrouwelijke data en voorkomt dat andere anti-spam gateways onze gebruikers blacklisten."

"FortiMail is voor ons een erg belangrijke toepassing," vult Mol aan. "We liggen de laatste maanden steeds meer onder vuur van ransomware, en de risico's daarvan zijn enorm. Met FortiMail worden deze aanvallen netjes tegengehouden. Bij het vorige product kwam er nog weleens wat doorheen, en nu niet. Daaraan zien we al dat Fortinet de verwachte resultaten waarmaakt."

FortiAuthenticator
De GGD werkt ook met dubbele authenticatie van gebruikers door middel van de tokens van FortiAuthenticator (200 licenties). "Dat werkt prima, maar het is uitdagend om mensen daarin mee te krijgen," vertelt Van de Paal. "Het is een extra handeling en het is nieuw, dus kan er weerstand bij de eindgebruikers onstaan. De uitrol van deze functionaliteit gaat daarom gecontroleerd en gefaseerd. We besteden veel aandacht aan het creëren van bewustzijn over waarom men het moet doen. We willen onze mensen erbij betrekken, anders heeft men het gevoel dat het wordt opgelegd."

Het is altijd zoeken naar de juiste balans tussen gebruikersgemak en beveiliging, weet ook Mol. "Er moet een compromis zijn tussen wat de organisatie wil en wat de eindgebruikers willen. Met geven en nemen komt er dan een oplossing uit."

De implementatie

De implementatie van het portfolio aan producten van Fortinet vond plaats in twee delen: de eerste fase bestond uit de installatie en configuratie van de FortiGate-appliances en van FortiAnalyzer. "Vervolgens hebben we zelf de overige oplossingen van Fortinet geïnstalleerd voor de laptops," vertelt Van de Paal. "Dat wijst zichzelf en is met een klein beetje finetunen zo gebeurd. We hebben 4IP gevraagd om de centrale beheeromgeving op te zetten zodat onze beheerders er altijd bij kunnen. Een nieuwe implementatie is lastig om helemaal zelf te doen, dus we waren blij dat we op de hulp van 4IP konden vertrouwen. Het uitvoeren van updates en aanpassingen is echter heel gemakkelijk en onze medewerkers konden na een korte training snel aan de slag met het beheer."

De overstap van de oude naar de nieuwe omgeving vond, weliswaar gecontroleerd, in één keer plaats. Mol: "Dat was wel spannend, maar het verliep uitstekend. We hebben het slim aangepakt door de dingen eerst vrij ver open te zetten om te zien wat er allemaal doorheen gaat. Vervolgens hebben we alles gaandeweg verder dichtgedraaid. Dat verliep heel gecontroleerd en nam maar een korte periode in beslag. Alles werd verder offline geconfigureerd en we zijn wat de ruleset van de firewall betreft met een schone lei begonnen. Deze is helemaal opnieuw opgebouwd."

De implementatie van FortiMail was de hekkensluiter van het project. "Je kan zelf regelen wat FortiMail door moet laten, er stond aanvankelijk teveel dicht," vertelt Van de Paal. "De grootste moeilijkheid zijn nieuwsbrieven, want de een wil ze wel, de ander niet. Dat is lastig in te schatten. Nu houden we nieuwsbrieven op verzoek tegen, daarvoor liet het systeem

alles door. Dat is een mooie oplossing, die wel handmatig bereikt moet worden. Daar ging behoorlijk wat tijd in zitten, maar nu gaat alles goed. De servicedesk regelt nu wat er wel en niet door gaat naar de gebruikers."

De voordelen

Nu de GGD Brabant Zuidoost enig tijd werkt met de oplossingen van Fortinet valt het vooral op hoeveel verkeer er tegengehouden wordt. Mol: "Zelfs websites waarvan je in eerste instantie denkt waarom worden deze gezien als malware? Dan blijkt er toch een omleiding in te zitten naar een malwaresite of een javascript dat verdacht is."

Jurgen Mol: "We hebben geen omkijken meer naar de IT-beveiliging en deze is meer up-to-date dan ooit. Het is vooral prettig dat het systeem real-time en proactief werkt. Het grootste voordeel is echter dat alle producten volledig samenwerken en eenvoudig beheerd kunnen worden vanuit één console. Doordat elk component individueel presteert wordt het risico gespreid, en zo zijn we verzekert van een flexibele beveiliging dat het systeem optimaal beschermt."

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480