



“Die einzelnen Fortinet-Komponenten spielen sehr gut zusammen und bilden zusammen eine Sicherheitsarchitektur, die mit den neuen, hochentwickelten Bedrohungen Schritt hält.”

- Christoph Schneider,
Netzwerksicherheits- und
Datenschutzverantwortlicher,
Klinikum Fulda

Klinikum Fulda trotz Locky & Co. mit Advanced Threat Protection Framework von Fortinet

Zum Schutz vor immer ausgefeilteren Sicherheitsbedrohungen hat das Klinikum Fulda seine vorhandene Security-Infrastruktur erweitert. Neben Next Generation Firewall und Secure E-Mail Gateway gehört dazu heute auch eine Sandbox-Lösung von Fortinet. Die Infrastruktur, die gemeinsam mit dem IT-Partner VINTIN implementiert wurde, schützt damit auch vor Zero-Day-Attacken und Ransomware wie Locky & Co.

Das Klinikum Fulda ist das moderne und leistungsstarke Krankenhaus der Maximalversorgung in Osthessen. Mit mehr als 1.000 Betten in der stationären Versorgung und einem breiten Angebot an spezialisierten Sprechstunden sowie Ambulanzen stellt es die qualitativ hochwertige medizinische Versorgung für die mehr als 500.000 Bürgerinnen und Bürger der Region sicher.

Jedes Jahr werden in den Einrichtungen des Klinikums über 100.000 Patientinnen und Patienten behandelt – 40.000 davon stationär – und von mehr als 2.700 hochqualifizierten Mitarbeiterinnen und Mitarbeitern betreut. Die 25 Kliniken und Institute bieten in fachabteilungsübergreifenden Zentren medizinische Leistungen mit modernsten Behandlungsmethoden, die auch den Vergleich mit Universitätsklinika standhalten.

Als Campus Fulda der Universitätsmedizin Marburg ist das Klinikum Fulda in die neuesten Entwicklungen der medizinischen Forschung eingebunden.

Eckdaten

Kunde: Klinikum Fulda

Branche: Gesundheitswesen

Standort: Fulda

Nutzungsszenario: Absicherung des Netzwerks eines modernen Krankenhauses

Vorteile

- Aufbau einer ganzheitlichen Sicherheitsinfrastruktur
- Zuverlässige Abwehr bekannter und neuer Gefahren
- Sichere Integration von Systemen im Bereich der Medizintechnik
- Hervorragende Performance und Skalierbarkeit
- Sichere Kommunikation zwischen den verschiedenen Netzwerksegmenten

Hochleistungsmedizin setzt sichere IT-Systeme voraus

Ohne moderne IT-Systeme ist das vielfältige Behandlungsangebot im Klinikum Fulda heute nicht mehr vorstellbar. Daher müssen auch die Sicherheitslösungen zum Schutz der IT-Infrastruktur höchste Anforderungen erfüllen. Die IT-Organisation des Klinikums sieht dabei aktuell vor allem drei Herausforderungen: „Zum einen nehmen wir neuartige Bedrohungen wie Ransomware sehr ernst und benötigen entsprechende Schutzmaßnahmen“, sagt Diplom-Informatiker Christoph Schneider, der in der IT-Abteilung des Klinikums für Netzwerksicherheit und Datenschutz verantwortlich ist.

„Eine weitere Herausforderung ist die sichere Integration von Systemen im Bereich der Medizintechnik. Hier geht es darum, die medizintechnischen Geräte vom übrigen Netzwerk abzuschotten und gleichzeitig den im Gesundheitswesen geforderten Datenaustausch zu ermöglichen. Und schließlich müssen wir uns mit einem veränderten Benutzerverhalten auseinandersetzen. Anwender nutzen die Möglichkeiten der Informationstechnologie heute ganz selbstverständlich im Privatleben, ohne sich Gedanken über Sicherheit und Datenschutz zu machen. Dies müssen wir bei der Planung unserer Security-Strategie ebenfalls berücksichtigen.“

Die IT-Organisation des Klinikums Fulda investiert daher nicht nur in leistungsfähige Sicherheitstechnologien, sondern setzt auch konsequent auf Awareness-Maßnahmen, um die Anwender für mögliche Risiken zu sensibilisieren: „Wir haben unseren Mitarbeitern beispielsweise erklärt, warum Web-Mail-Dienste und Filesharing-Services wie Dropbox im internen Netzwerk gesperrt sind“, sagt Christoph Schneider. „Uns ist wichtig, dass sie verstehen, welche Gefahren von diesen Diensten für die Sicherheit unseres Netzwerks ausgehen können.“

FortiGate-Cluster vereint unterschiedliche Security-Technologien

Gleichzeitig hat die IT-Abteilung mit Unterstützung des IT-Dienstleisters VINTIN eine ganzheitliche Sicherheitsinfrastruktur aufgebaut, die sowohl bekannte als auch neuartige Gefahren zuverlässig abwehrt. Ein zentraler Baustein der Security-Architektur ist das hochverfügbare FortiGate 1200D-Cluster in den beiden Rechenzentren des Klinikums.

Die leistungsfähigen Next Generation Firewalls von Fortinet schützen die IT-Umgebung in Echtzeit vor Netzwerk- und Content-basierenden Bedrohungen. Neben marktführender Firewall-Technologie vereinen die Appliances auf einer Plattform unterschiedliche Sicherheitskomponenten wie zum Beispiel Anti-Malware, VPN, Intrusion Prevention und Web-Filtering. Zudem zeichnet sich die FortiGate-Plattform durch herausragende Performance und Skalierbarkeit aus. Speziell entwickelte FortiASIC-Prozessoren beschleunigen Funktionen wie das Content Scanning und sorgen dafür, dass hohe Netzwerksicherheit nicht zu Lasten des Datendurchsatzes geht.

Anfang 2016 hat VINTIN die aktuellen FortiGate-Systeme im Klinikum Fulda implementiert. Die neuen Appliances verfügen bereits über 10 GbE-Interfaces und bieten damit auch die benötigte Bandbreite für die interne Netzwerkabsicherung.

„Wir setzen die FortiGate-Systeme auch als interne Firewalls ein und haben so Netzwerksegmente für die Medizintechnik und die Haus- und Gebäudetechnik vom übrigen IT-Netzwerk getrennt“, erklärt Christoph Schneider. „Mit dieser LAN-Segmentierung kommen wir heute bereits den Anforderungen des neuen IT-Sicherheitsgesetzes nach und bieten zusätzlichen Schutz für kritische medizintechnische Geräte. Die FortiGate-Systeme ermöglichen eine sichere Kommunikation zwischen den verschiedenen Netzwerksegmenten – ohne Einbußen bei der Performance.“

Ein weiterer Baustein in der Sicherheitsarchitektur des Klinikums ist das Secure E-Mail-Gateway FortiMail, auch beim Schutz vor Spam-Mails und Malware, die via E-Mail verbreitet wird, entschieden sich die IT-Verantwortlichen für eine Fortinet-Lösung. Neben der einheitlichen Benutzeroberfläche und dem umfassenden Funktionsumfang war dabei das nahtlose Zusammenspiel mit der FortiGate-Plattform ausschlaggebend.

Wenn die FortiMail-Lösung einen Absender von Spam-Mails identifiziert, wird diese Information automatisch an das FortiGate-System weitergegeben und die Adresse ab sofort geblockt. Die FortiMail-Lösung filtert aber nicht nur Spam-Mails aus dem eintreffenden E-Mail-Verkehr, sondern überprüft auch die ausgehenden E-Mails. Outbound Inspection-Technologien von Fortinet verhindern, dass potentielle Schadsoftware über die E-Mail-Server des Klinikums versendet wird – und die Organisation so auf den Blacklists anderer Gateways landet.

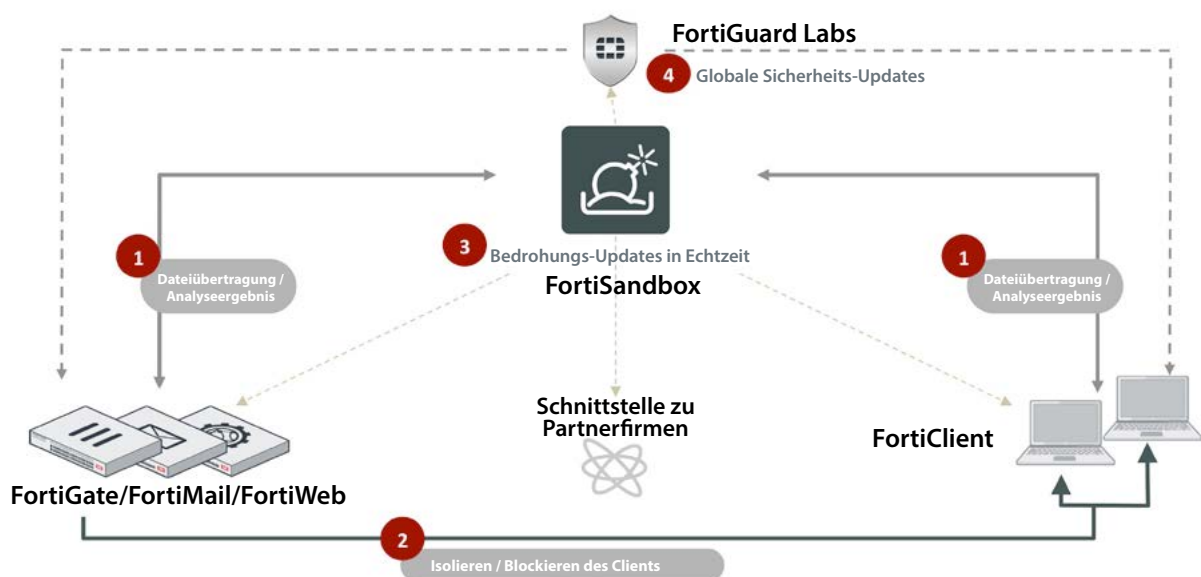
Sandbox-Lösung zum Schutz vor Ransomware

„FortiMail fängt Spam und E-Mails mit bekannter Malware sehr zuverlässig ab, bietet allerdings keinen vollständigen Schutz vor hochentwickelten E-Mail-Bedrohungen“, berichtet Christoph Schneider. „Für die Abwehr von Ransomware und anderen neuartigen Attacken wurde uns der Einsatz einer FortiSandbox empfohlen.“

Die Sandbox-Lösung von Fortinet analysiert verdächtige Dateien wie Office-Dokumente, PDFs oder ZIP-Archive in einer geschützten Umgebung und gibt nur unbedenkliche Dateien für den Anwender frei. Schädliche Elemente werden automatisch blockiert und entsprechende Warnungen an das Sicherheits-Ökosystem von Fortinet übermittelt. FortiSandbox schützt damit sehr effektiv vor Zero-Day-Attacken und anderen Angriffen, die von traditionellen Sicherheitslösungen nicht entdeckt werden.

„Viele Attacken auf unser Netzwerk sind mittlerweile ausgesprochen raffiniert getarnt“ sagt Christoph Schneider. „Vor kurzem erreichte uns beispielsweise per E-Mail ein Bewerbungsschreiben mit einem angehängten Lebenslauf. Die Analyse in der Sandbox-Umgebung zeigte, dass es sich bei dem Attachment nicht um ein PDF-File, sondern um eine mit Malware verseuchte Datei handelte. Die FortiSandbox blockierte den Anhang und verhinderte so, dass ein Anwender das Attachment versehentlich öffnet und so unser Netzwerk mit Schadcode infiziert.“

Die FortiSandbox arbeitet nicht nur mit FortiMail zusammen, sondern lässt sich auch mit der FortiGate-Plattform verbinden. Auf diese Weise können beispielsweise auch sämtliche Web-Downloads proaktiv auf verdächtige Dateien überprüft werden. Wenn die Sandbox-Lösung dabei Malware identifiziert, werden die Web-Filter des FortiGate-Clusters automatisch angepasst.



Sicherheitsarchitektur hält mit wachsenden Anforderungen Schritt

Um die Leistung der FortiSandbox bei Bedarf flexibel skalieren zu können, wurde die Lösung als virtuelle Appliance im Rechenzentrum des Klinikums implementiert. „Die Anfangsinvestition war dadurch für uns niedriger als bei einer physischen Appliance – und bei steigenden Anforderungen fügen wir einfach zusätzliche Serverressourcen hinzu“, sagt Christoph Schneider. „Zusätzlich profitieren wir von erhöhter Ausfallsicherheit, da wir die virtuelle Appliance sehr schnell im laufenden Betrieb auf andere Hardware verschieben können.“

Der IT-Experte sieht das Klinikum Fulda mit den implementierten Technologien sehr gut für die aktuellen Sicherheitsanforderungen gewappnet: „Die einzelnen Fortinet-Komponenten spielen sehr gut zusammen und bilden zusammen eine Sicherheitsarchitektur, die mit den neuen, hochentwickelten Bedrohungen Schritt hält. Zudem haben wir mit FortiAnalyzer eine zentrale Lösung für Logging und Reporting eingerichtet. Damit haben wir alle Sicherheitsthemen immer im Blick und können jederzeit individuelle Analysen und Berichte erstellen, die uns bei der Weiterentwicklung unserer Security-Strategie helfen.“



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428