Security mit Fortinet

Krankenhaus-IT und -OT ganzheitlich schützen

Cyberangriffe auf das Gesundheitswesen nehmen zu. Mit der Bedrohungslage steigen auch die Anforderungen an die Security. Noch bis Ende April haben Kliniken Zeit, das IT-SIG 2.0 umzusetzen. Doch Fachkräftemangel und schwer abzusichernde Medizintechnik sind eine Herausforderung für sich. Außerdem sollten neben den neuen Anforderungen auch die bestehenden Hausaufgaben nicht außer Acht gelassen werden. Mit der ACP Secure Fabric und Fortinet können Sie wieder ruhig schlafen – und Fördermittel des KHZG richtig einsetzen.

IT for innovators.

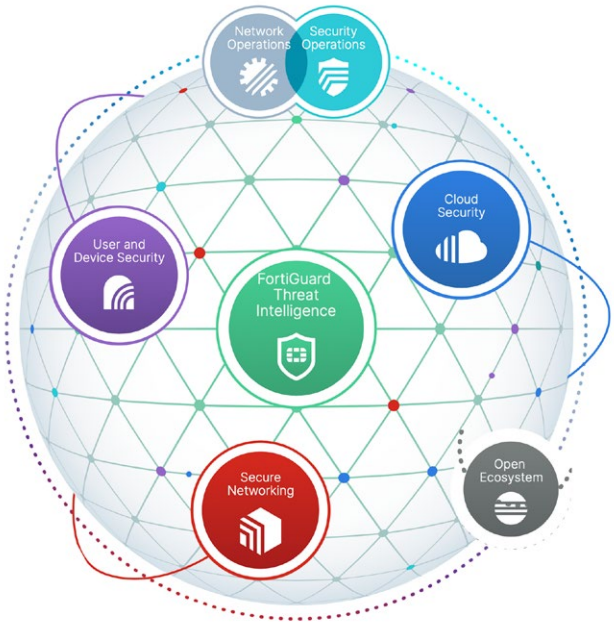
Was ist Ihre Sicherheits-Strategie?

Als IT-Verantwortlicher im Krankenhaus haben Sie keinen leichten Job. Mit einem kleinen Team, das ohnehin am Anschlag arbeitet, müssen Sie wachsende Sicherheits-Anforderungen erfüllen. Aber wie? Security-Expert*innen sind auf dem Arbeitsmarkt schwer zu finden, und die Lage ist so angespannt wie nie.

Seit 2019 haben Angriffe auf Gesundheitseinrichtungen um 200 Prozent zugenommen, so der NTT Global Threat Intelligence Report. Allein im vergangenen halben Jahr wurden vier Vorfälle bei deutschen Krankenhäusern gemeldet. Die Dunkelziffer dürfte deutlich höher sein. Längst haben Cyberkriminelle das Gesundheitswesen als attraktives Ziel entdeckt. Denn hier sind die Chancen besonders gut, dass die Opfer Lösegeld zahlen. Ohne IT stehen keine Patientendaten zur Verfügung, können keine Laboruntersuchungen durchgeführt werden und funktionieren medizintechnische Geräte nicht. Daher ist der Druck hoch, die Systeme am Laufen zu halten. So manches Klinikum, das verschlüsselt wurde, geht lieber auf die Forderungen der Hacker ein, als einen langen Stillstand zu riskieren.

Rundum geschützt mit ACP und Fortinet

Klar ist: Eine Firewall allein reicht nicht aus, um den Hackern Paroli zu bieten. Gesundheitseinrichtungen brauchen heute Security-Lösungen auf allen Ebenen der IT-Umgebung – vom Endpunkt über das Netzwerk und E-Mail bis hin zur Cloud. Diese müssen zusammenarbeiten und Daten austauschen, damit ein 360°-Blick entsteht. Hier spielt die Fortinet Security Fabric ihre Stärke aus: Sie vereint Lösungen für alle wichtigen Sicherheitsfunktionen unter einer einheitlichen Plattform mit zentralem Management. Die führende Sicherheitstechnologie kommt im Rahmen der ACP Secure Fabric zum Einsatz – unserem Framework für Ihre ganzheitliche Security-Strategie.



Mit der Fortinet Security Fabric sind Sie bestens für die Anforderungen des IT-Sicherheitsgesetzes 2.0 gerüstet. Die meisten Fortinet-Lösungen sind förderungsfähig nach dem KHZG.

Die Uhr tickt

IT SIG 2.0

- Bis Ende April haben KRITIS-Betreiber noch Zeit, die Maßnahmen für das IT-SIG 2.0 umzusetzen.
- Andernfalls drohen Bußgelder.
- Auf technischer Seite bedeutet das: Sie müssen Systeme zur Angriffserkennung implementieren.

KHZG

- Mit dem Krankenhauszukunftsgesetz stellt der Bund insgesamt 4,3 Milliarden Euro für die Digitalisierung bereit.
- 15 Prozent der Fördermittel müssen für die IT Security eingesetzt werden.
- Wer Fördergelder beantragt hat, muss bis Sommer 2023 die gesetzlich geforderten digitalen Dienste und Sicherheitseinrichtungen bereitstellen.
- Sonst drohen Abschläge von bis zu 2 Prozent der Rechnungsbeträge für alle voll- und teilstationären Fälle.

KHZG-förderungsfähig

Medizintechnische Geräte schützen mit FortiGate

Herausforderung

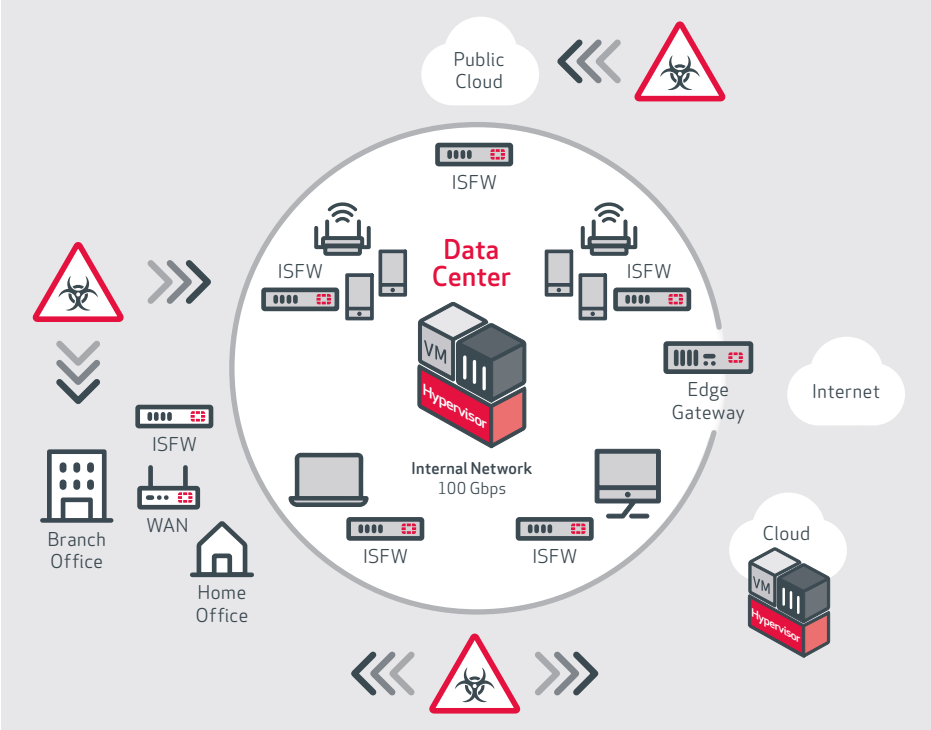
Die Medizintechnik ist das Sorgenkind der IT Security. Denn die Geräte arbeiten häufig mit veralteten Betriebssystemen, die sich weder updaten noch patchen lassen. Sie mit Endpunkt-Security zu schützen, ist nicht möglich. Für Cyberkriminelle sind die offenen Schwachstellen geradezu eine Einladung. Mittlerweile gibt es sogar Ransomware, die speziell für OT-Systeme entwickelt wurde. Angreifen lassen sich diese über viele verschiedene Vektoren. Denn Bedrohungen können nicht nur von außen, sondern auch von innen kommen, etwa mobilen Endgeräten von Patienten, die sich bereits im Netzwerk befinden.

Lösung

Mit der FortiGate Next Generation Firewall können Sie das Netzwerk segmentieren und Legacy-Systeme in einer eigenen, gesicherten Zone betreiben. An jeder Zonengrenze finden dann Kontrollen statt und werden Richtlinien umgesetzt, um Benutzer, Anwendungen und den Datenfluss zu steuern. So können Cyberkriminelle nicht mehr ungehindert vordringen. FortiGate ermöglicht kleinste Mikrosegmentierung. Dabei arbeitet sie so schnell, dass der Datenfluss nicht gestört und die Performance von Applikationen nicht beeinträchtigt wird.

Fortinet wurde zum wiederholten Mal im Gartner Magic Quadrant für Netzwerk Firewalls 2022 und im Forrester Wave „Enterprise Firewalls“ Q4 2022 als Leader genannt und zählt seit vielen Jahren zu den führenden Security-Herstellern.

Mit FortiGate erfüllen Sie folgende B3S-Anforderungen nach IT SIG 2.0: 7.13.1 ANF-MN 93&94, 7.13.2 ANF-MN 95,96,97



Ihre Vorteile

- Durchgängige ultraschnelle Sicherheit
- Makro- und Mikrosegmentierung
- Volle Transparenz mit SSL-Inspektion, einschließlich TLS 1.3
- Konsistenter Echtzeitschutz mit FortiGuard-Diensten
- Hervorragende Nutzererfahrung mit Security Processing Units
- Operative Effizienz und automatisierte Workflows
- Nativ integrierter Proxy
- Bester ROI in der Branche

Netzwerksicherheit mit Fortinet im Krankenhaus Agatharied

Das Krankenhaus Agatharied hat mit Fortinet und ACP Rundum-Schutz vor aktuellen Bedrohungen etabliert. Es kombiniert FortiGate mit FortiMail und FortiSandbox.

Lesen Sie HIER > die Kundenreferenz.

KHZG-förderungsfähig

Angreifer täuschen mit FortiDeceptor

Herausforderung

Cyberangriffe bleiben oft lange unbemerkt. Bis es zur Verschlüsselung kommt, können Monate vergehen. Während dieser Zeit spionieren Cyberkriminelle in aller Ruhe das Netzwerk aus, suchen nach den wertvollsten Daten und laden Malware nach. Reaktive Security-Lösungen greifen oft zu spät. In der Regel konzentrieren sie sich entweder auf externe oder interne Bedrohungen, aber nicht auf beides.

Lösung

Mit FortiDeceptor können Sie ein proaktives Honeypot-System aufbauen, das externe und interne Angreifer täuscht und in die Falle lockt. Es rollt automatisiert Deception-VMs und Decoys aus, die sich in Ihre Infrastruktur integrieren. Dabei kann FortiDeceptor sogar medizintechnische Geräte simulieren. Indem Sie den Honeypot so platzieren, dass er als Erstes angegriffen wird, erhalten Sie ein Frühwarnsystem. Sie können Eindringlinge in Quarantäne nehmen, untersuchen und Schwachstellen schließen, bevor Schaden entsteht.

> „Indem wir FortiDeceptor Bedrohungen aussetzen, die andernfalls unsere kritischen Systeme treffen könnten, erhalten wir ein echtes Bild davon, was unsere extern zugänglichen Server täglich durchmachen."
>
> CIO, Regional Hospital System

Ihre Vorteile

- Proaktive Security: Vorsorge statt Nachsorge
- Honeypot, der sogar medizintechnische Geräte vortäuschen kann
- Automatische Erkennung und Reaktion auf externe und interne Bedrohungen
- Wirkt wie kontinuierliches Pentesting

KHZG-förderungsfähig

Zero-Day-Bedrohungen erkennen mit FortiNDR

Herausforderung

Die Frequenz und Häufigkeit, mit der Unternehmen angegriffen werden, nimmt rasant zu. Gleichzeitig entwickeln Cyberkriminelle immer komplexere Malware. Neue Bedrohung zu erkennen, ist schwer. Zumal Security-Teams von der Masse an Warnmeldungen, die sie überwachen und auswerten müssen, geradezu erschlagen werden.

Lösung

FortiNDR überwacht den Netzwerkverkehr mithilfe von Deep Learning, analysiert Dateien und untersucht Infektionsquellen. Die Analysen erfolgen erheblich schneller als bei einer Sandbox. Da das System kontinuierlich dazulernt, kann es auch Zero-Day-Bedrohungen aufdecken. Ein virtueller Security Analyst minimiert die Zahl der False Positives und entlastet SOC-Mitarbeiter*innen, sodass sie sich sofort auf das Wesentliche konzentrieren können.

Ihre Vorteile

- Bedrohungen schneller erkennen und reagieren
- Malware-Klassifizierung in weniger als einer Sekunde
- Bewährte KI, trainiert mit mehr als 6 Millionen Malware-Erkennungsfunktionen
- Einheitlicher Schutz vor IT/OT-Zero-Day-Bedrohungen

Lassen Sie sich unterstützen!

Welche Fortinet-Lösungen am besten für Ihre Klinik geeignet sind, hängt von Ihren individuellen Anforderungen und Ihrer Security-Strategie ab. Wo haben Sie noch Lücken? Wohin möchten Sie sich in den nächsten drei bis fünf Jahren entwickeln? Das sind entscheidende Fragen, die wir gerne gemeinsam mit Ihnen klären. Sprechen Sie uns an!

Managed Services sind unverzichtbar

Leistungsfähige Security-Technologie ist nur die halbe Miete – man muss sie auch richtig konfigurieren, betreiben und monitoren. Wer überwacht die Warnmeldungen, die die Systeme ausgeben, und wer wertet sie aus? All das erfordert spezialisiertes Know-how, das man nicht mal schnell in ein paar Monaten aufbaut. Kaum eine Klinik hat genügend Security-Expert*innen im Team. Sie selbst auszubilden dauert Jahre, und dann wandern die Spezialist*innen womöglich in die Industrie ab, weil sie dort höhere Gehälter erzielen.

ACP verfügt über langjährige Erfahrung im Security-Umfeld von Krankenhäusern und wurde vielfach als **„Fortinet Partner of the Year“** ausgezeichnet. Wir unterstützen Sie dabei, eine ganzheitliche Security-Strategie zu entwickeln, die passenden Produkte auszuwählen, zu implementieren und zu betreiben. So entlasten Sie Ihre IT-Abteilung und schlagen dem Fachkräftemangel ein Schnippchen.

Unser Tipp:
Lagern Sie Infrastrukturthemen aus

Der Fachkräftemangel spitzt sich weiter zu. Umso wichtiger wird es, gut mit den eigenen Ressourcen zu haushalten. Verlagern Sie Ihre Mitarbeiter*innen auf die Bereiche, die Sie nur schwer outsourcen können – etwa die Applikationsbetreuung. Infrastruktur-Themen wie das Firewall-Management lassen sich dagegen leicht in einen Managed Service auslagern.

„In der Security sagen wir immer: Sei besser als dein Nachbar – dann greifen die Hacker nicht dich an, sondern ihn.“

Lars Buschkamp
Business Development Manager Healthcare,
ACP Holding Deutschland GmbH

Einfach für Sie da.

ACP Holding Deutschland GmbH
healthcare@acp.de
www.acp.de/focus/healthcare

FORTINET