SOLUTION BRIEF

Vollständige Transparenz und zentrale Kontrolle über OT-Umgebungen erreichen

Zusammenfassung

Die Konvergenz von Informationstechnologie (IT) und Betriebstechnologie (OT) führt zu einer erweiterten OT-Angriffsfläche. Security, Ausfallsicherheit und Betriebsschutz lassen sich immer schwerer aufrechterhalten – der Druck auf Network-Operations-Analysten steigt. Betriebstechnologie erfordert heutzutage eine integrierte Security-Infrastruktur, um Transparenz, Kontrolle und Einblick in den Kontext von Geräten zu gewährleisten und die Anfälligkeit dieser Geräte für wachsende, neue Bedrohungen aus dem Internet zu kennen. Die Fortinet Security Fabric bietet eine durchgängige Security-Architektur für OT-Umgebungen mit einem integrierten, automatisierten Schutz, der durch Segmentierung, Netzwerk-Zugangskontrolle (NAC) und SIEM (Security Information and Event Management) erreicht wird.

Fast Dreiviertel der OT-Unternehmen haben in den letzten 12 Monaten einen Malware-Angriff erlebt, der Schäden für Produktivität, Ertrag, Markenvertrauen, geistiges Eigentum und die physische Sicherheit nach sich zog.[1]

78 % der OT-Unternehmen haben Berichten zufolge nur eine teilweise zentralisierte Transparenz über die Cyber-Security-Lösungen in ihren OT-Umgebungen.[4]

Mehr Transparenz, Kontrolle und Kontextinformationen sind notwendig

Die OT-Angriffsfläche erweitert sich schnell. Wichtige Systeme in kritischen Infrastrukturen und Industrieumgebungen sind zunehmend durch Infrastrukturänderungen gefährdet, wenn beispielsweise serielle OT-Verbindungen durch digitale Verbindungen ersetzt werden. Aber auch der rasante Anstieg bei mit dem Internet verbundenen Geräten verschärft die Bedrohungslage zusehends.

Ungeachtet all dieser Herausforderungen müssen Network-Operations-Analysten dafür sorgen, dass die betriebliche Ausfallsicherheit und der Betriebsschutz jederzeit gegeben sind. Problematisch ist nur, dass die Cyber-Security von OT-Umgebungen oft vernachlässigt wird. Schuld daran ist der sogenannte „Air Gap“ – der schützende Luftspalt, der OT- und IT-Systeme bislang trennte und so Betriebstechnologie sicher vor Bedrohungen abschirmte. Diese Trennung fällt zunehmend weg, wodurch OT-Systeme plötzlich z. B. für Malware anfällig werden, die nach E-Mail-Phishing-Kampagnen über IT-Verbindungen in OT-Netzwerke gelangt.[2,3]

Der Priorisierung der OT-Security wird in letzter Zeit viel Aufmerksamkeit gewidmet. Allerdings lassen sich herkömmliche IT-Sicherheitsstrategien nicht einfach auf Betriebstechnologie übertragen, die meistens aus vielen störempfindlichen – und oft veralteten – Systemen besteht. Um einen sicheren, funktionalen Betrieb aufrechtzuerhalten, benötigen Unternehmen daher drei wichtige Cyber-Security-Funktionen:

Transparenz

Der Schutz moderner OT-Umgebungen beginnt mit dem Aufbau einer kontinuierlichen Transparenz über jede Ressource, die mit dem Netzwerk verbunden ist. Alles muss einbezogen werden: kabellose und drahtlose Verbindungen. Die Security muss zudem sämtliche verbundenen Geräte unternehmensweit verfolgen können – z. B. wann sie sich mit dem Netzwerk verbinden, wann sie das Netzwerk verlassen oder wenn ein Ortswechsel stattfindet.

Steuerung

Unternehmen müssen Zugriffsrichtlinien präzise für Geräte und Benutzer abstimmen, anwenden und durchsetzen können, um den OT-Betrieb vor potenziellen IT-basierten Bedrohungen zu schützen. Dynamische, rollenbasierte Steuerungen können Anwendungen gruppieren, Daten verknüpfen und den Zugriff auf bestimmte Gruppen begrenzen, um den OT-Bedrohungsschutz zu stärken. Diese Form der absichtsbasierten Segmentierung bietet eine feinmaschige Kontrolle, die den Zugriff nach einer ständig neuen Vertrauensbewertung für Geräte und Benutzer anpasst.

Lageerkennung

Wird ein Gerät in einer OT-Umgebung angegriffen, muss sofort ein Alarm ausgelöst werden und der Bedrohungskontext einsehbar sein. Nur dann kann das Security-Team schnell die richtigen Maßnahmen ergreifen und die Sicherheitsverletzung eingrenzen. Für den Schutz von Betriebstechnologie sind eine einheitliche Ereigniskorrelation und ein besonderes Risiko-Management nötig, um Analysen zu beschleunigen, die Bedrohungsabwehr zu automatisieren und Sicherheitslücken schneller schließen zu können. Das gilt umso mehr angesichts personell begrenzter Security-Teams in den meisten Unternehmen.

Über die Hälfte der Unternehmen (53 %) hat keine interne Netzwerk-Segmentierung, um die Ausbreitung von Bedrohungen in OT-Netzwerken zu verhindern.[5]

Infolge des weltweiten Fachkräftemangels im Bereich Cyber-Sicherheit sind heute fast 3 Millionen Security-Positionen unbesetzt.[6]

Integrierte Security-Architektur für Betriebstechnologie

Die **Fortinet Security Fabric** verbindet verschiedene, in einer OT-Umgebung implementierte Sicherheitslösungen zu einem koordinierten Security-System. Diese integrierte Sicherheitsarchitektur koordiniert die Cyber-Bedrohungsabwehr im gesamten Unternehmen mit einer lückenlosen Transparenz, Kontrolle und Lageerkennung. Die Security Fabric bietet einen hochwirksamen Schutz für heutige OT-Umgebungen, weil sie das gesamte Unternehmen abdeckt und Funktionen umfasst, mit denen sich Sicherheitsprobleme schnell erkennen und beheben lassen.

Für OT-Umgebungen umfasst die Security Fabric mehrere Lösungen von Fortinet. Dazu gehören robuste **FortiGate** Next Generation Firewalls (NGFWs), sicheres Switching mit dem **FortiSwitch** (LAN) und **FortiAP** (WLAN), ein Endpunkt-Schutz mit dem **FortiClient** und eine zentrale Verwaltung aller unternehmensweit implementierten Geräte mit dem **FortiManager**.

Die Fortinet Security Fabric verbessert auch die Zugriffskontrolle auf kritische Systeme, ohne deren Betrieb zu stören. Traditionell wird bei der Zugriffskontrolle von unveränderlichen Vertrauensstufen für Benutzer, Geräte und Anwendungen ausgegangen. Tatsächlich ändert sich die Vertrauenswürdigkeit von Benutzern und Geräten jedoch häufig, z. B. durch Änderungen im Geschäftsbetrieb oder neuartige Bedrohungen. Bei der **absichtsbasierten Segmentierung** ist die Zugriffskontrolle deshalb an kontinuierlich aktualisierte Vertrauensstufen gebunden, deren Bewertung auf Informationen aus internen und externen Quellen basiert.

Konkret bedeutet das: Die absichtsbasierte Segmentierung von Fortinet unterstützt eine dynamische, granulare Zugriffskontrolle, die kontinuierlich die Vertrauensstufen von Benutzern überwacht und Sicherheitsrichtlinien entsprechend anpasst. Analysen und Automatisierung ermöglichen die Isolierung kritischer Ressourcen, um Bedrohungen schnell zu erkennen und proaktiv zu verhindern. Bereitgestellt wird die absichtsbasierte Segmentierung mit **FortiGate NGFWs**, die den Ost-West- und Nord-Süd-Datenverkehr in OT-Netzwerken von End-to-End kontrollieren.

Eine OT-Security ist jedoch wenig sinnvoll, wenn dadurch der Betrieb kritischer Systeme gestört oder sogar unterbrochen wird. Dank Investitionen in eine dedizierte OT-Security-Architektur verfügt Fortinet nachweislich über betriebstechnische Kompetenz: Fortinet-Lösungen werden von Fachexperten entwickelt, die mit den besonderen Sicherheits- und Betriebsanforderungen dieser einzigartigen Umgebungen vertraut sind. Mit der Security Fabric erhalten Unternehmen eine Komplettlösung für einen End-to-End-Schutz – im Gegensatz zu Lösungen anderer Anbieter, die sich aus mehreren Einzelprodukten und -diensten zusammensetzen und oft nur gegen einen Angriffsvektor helfen.

Lösungen für eine tiefgreifende OT-Transparenz

Ein Endpunkt-Schutz verbessert die Transparenz und Kontrolle über Geräte in OT-Umgebungen. Die folgenden drei Security-Fabric-Komponenten spielen dabei eine entscheidende Rolle:

FortiSIEM

Eine effektive OT-Security erfordert sowohl Transparenz als auch Kontextinformationen, damit Network-Operations-Analysten so schnell wie möglich Alarme sichten, Geräte verfolgen und Probleme lösen können. Mit FortiSIEM lassen sich Sicherheitsereignisse bei Geräten verschiedener Anbieter angehen. Diese Multivendor-Lösung bietet eine zentrale, umfassende Transparenz für die Korrelation, automatisierte Abwehr und Beseitigung von Bedrohungen. Das entlastet nicht nur personell begrenzte Teams, sondern verbessert auch die Erkennung von Sicherheitsvorfällen.

FortiClient

FortiClient schützt Workstations und geschäftlich genutzte Privatgeräte von Mitarbeitern (BYOD) in OT-Umgebungen. Dieser kritische Endpunkt-Schutz umfasst zahlreiche Sicherheitsfunktionen wie Anti-Virus, Anti-Malware, Anti-Exploit, eine Web Application Firewall (WAF) und Web-Filter. Außerdem gibt es einen Fabric Agent für Telemetriedaten von Endgeräten, der den FortiClient in die FortiGate NGFW-Security einbindet.

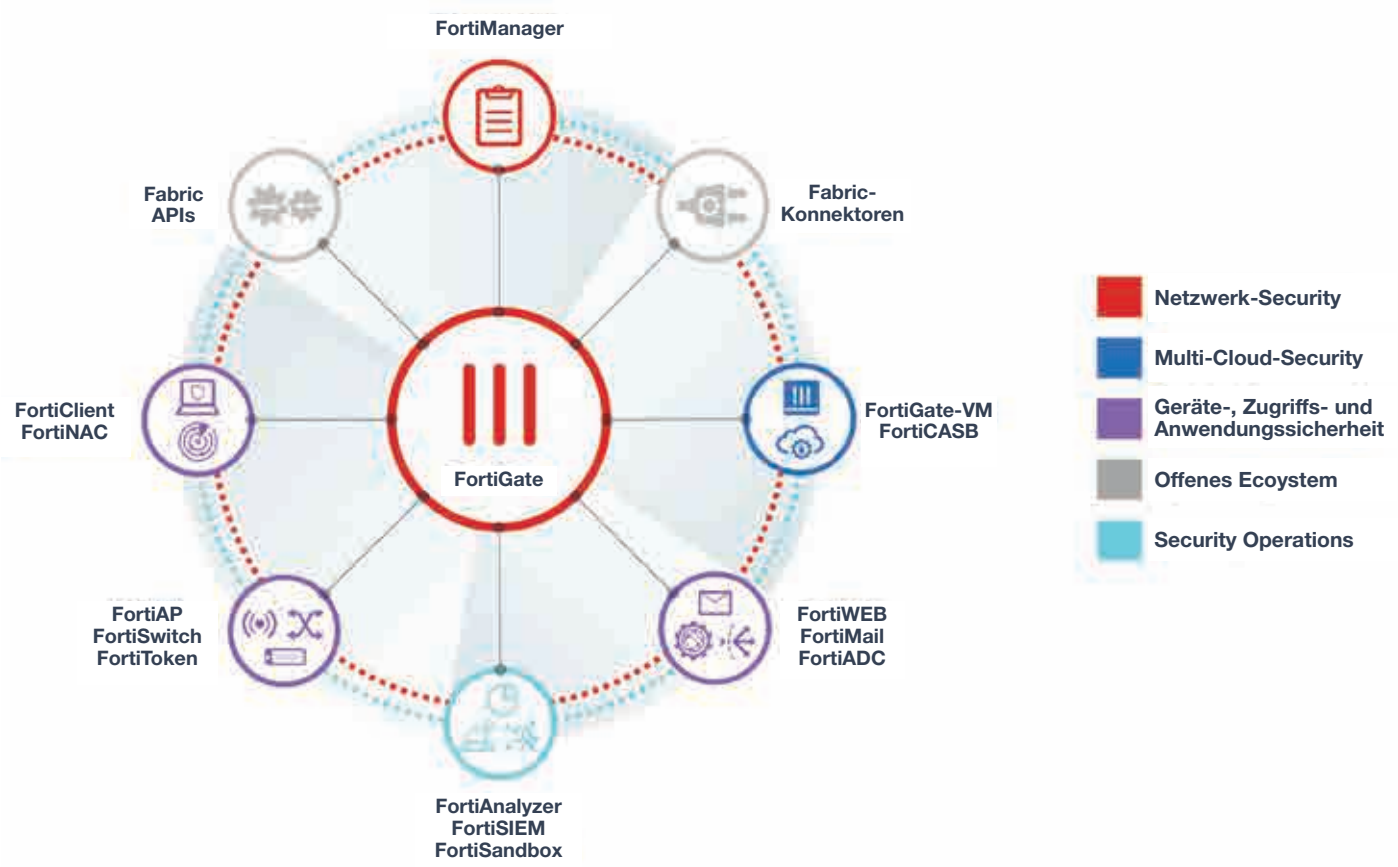
FortiNAC

FortiNAC verbessert den Schutz von OT-Geräten und -Systemen, die keine oder unzureichende Sicherheitsfunktionen haben – z. B. von IoT/IIoT-Geräten, speicherprogrammierbaren Steuerungen (SPS), Steuerungstechnik (ICS) und SCADA-Subsystemen. In Abstimmung mit anderen Security-Fabric-Lösungen unterstützt FortiNAC den Bedrohungsschutz stark dezentraler OT-Netzwerke, indem Endpunkte mit ungepatchten Schwachstellen erkannt werden.

Unkritische Endpunkte können sofort bis zum Patching automatisch aus dem Netzwerk entfernt und über das zentrale FortiNAC Dashboard auch wieder automatisch ins Netzwerk gebracht werden. Bei umfassenden Multivektor-Angriffen (z. B. Botnets) oder anderen Notfällen, bei denen der Zugriff aus Sicherheitsgründen streng begrenzt werden muss, lässt sich mit FortiNAC sogar das gesamte Netzwerk abriegeln. Will dann ein neues Gerät auf das Netzwerk zugreifen, muss dies manuell genehmigt werden.

Entscheiden Sie sich für eine Security speziell für Betriebstechnologie

Durch die Konvergenz von OT und IT müssen Network-Operations-Analysten jetzt anfällige OT-Systeme vor unzähligen Bedrohungen aus dem Internet schützen. Die Fortinet Security Fabric bietet dafür grundlegende Sicherheitsfunktionen, die speziell für OT-Umgebungen entwickelt wurden. Network-Operations-Analysten erhalten damit vollkommene Transparenz, richtlinienbasierte Steuerungen und eine sofortige Lageerkennung.



Die Fortinet Security Fabric bietet eine einheitliche, integrierte Sicherheitsarchitektur, die eine umfassende Automatisierung ermöglicht.

Die Security Fabric integriert spezielle Technologien (Segmentierung, SIEM, NAC, Endpunkt-Schutz, Switching und WLAN), um Betriebstechnologie vor der Flut an IT-basierten Bedrohungen zu schützen. Network-Operations-Analysten sollten ihre derzeitige OT-Security unter den folgenden Aspekten neu bewerten:

Kann meine OT-Security ...

- eine integrierte Security-Architektur nutzen, die alle Teile der Security-Architektur zu einem zusammenhängenden, kollektiven System verbindet?
- mehr Transparenz bei der OT-Netzwerk-Discovery bieten, um das aktuelle Sicherheitsprofil zu kennen?
- IoT- und IIoT-Geräte anhand von Risikofaktoren wie Schwachstellen, Sicherheitsbewertungen oder sogar Auslastung erkennen und kategorisieren?
- eine absichtsbasierte Segmentierung anwenden, um die Ausfallsicherheit von OT-Netzwerken zu verbessern?
- Lösungen wie SIEM und NAC einbinden, um verdächtige Benutzer und Geräte zu finden?
- Bedrohungsinformationen für eine Lageerkennung in Echtzeit nutzen, ohne dabei kritische Betriebsabläufe zu stören?
- das Security-Management durch eine zentrale Konsole vereinfachen?

[1] „State of Operational Technology and Cybersecurity Report“. Fortinet, März 2019.
[2] „DHS Alert ICS-ALERT-14-176-02A“. Cybersecurity and Infrastructure Security Agency, 22. August 2018.
[3] Catalin Cimpanu: „The Clever Phishing Trick Used by Hackers Targeting the US Energy Sector“. BleepingComputer, 10. Juli 2017.
[4] „State of Operational Technology and Cybersecurity Report“. Fortinet, März 2019.
[5] Ebd.
[6] „Cybersecurity Skills Shortage Soars, Nearing 3 Million“. (ISC)², 18. Oktober 2018.

FORTINET

www.fortinet.com/de

14. Dezember 2020, 15:43 Uh

360483-0-0-DE