SOLUTION BRIEF

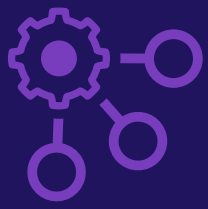
Fortinet schützt OT-Netzwerke vor hochkomplexen Bedrohungen

Zusammenfassung

Fortinet-Lösungen wurden speziell entwickelt, damit Unternehmen ihre Netzwerke für Betriebstechnologie (OT) und industrielle Steuerungstechnik (ICS) schützen und zugleich die Hochverfügbarkeitsanforderungen dieser Umgebungen erfüllen können. Fortinet-Lösungen umfassen eine strategische Security-Automatisierung sowie Deception-Technologien, um Angreifer in OT-Netzwerken schneller zu erkennen und zu entfernen. Mit einer Netzwerk-Segmentierung und Zugriffskontrolle werden laterale Angriffe eingedämmt, damit sich Angreifer nicht mehr quer durch das Netzwerk bewegen können, die Systemverfügbarkeit erhalten bleibt und nicht infizierte Geräte geschützt werden. Bedrohungsdaten speziell für Betriebstechnologie – bereitgestellt von den FortiGuard Labs und Fortinet-Partnern – liefern wichtige Einblicke und Kontextinformationen, die zum Identifizieren und Eliminieren von OT-Bedrohungen unverzichtbar sind.

Einleitung

Hochgefährliche Bedrohungsakteure versuchen immer häufiger, Zugang zu wertvollen, kritischen OT-Systemen zu erhalten. Doch der Schutz dieser nicht standardisierten – und oft veralteten Systeme – ist alles andere als einfach. Fortinet bietet dafür eine Lösung: Mit der Fortinet Security Fabric erhalten Unternehmen eine vollständig integrierte Sicherheit und Transparenz über die gesamte Security-Infrastruktur, die sich über eine einzige Konsole zentral verwalten lässt. Dies ist möglich, weil alle Fortinet-Lösungen mit dem gleichen Betriebssystem arbeiten, ergänzt durch ein offenes API-System für Drittanbieter. Dank der Fortinet Security Fabric können OT-Netzwerk-Betreiber mit Fortinet-Lösungen hochkomplexe Bedrohungen schnell identifizieren, eindämmen und entfernen. Zu den Security-Funktionen gehören eine automatisierte Bedrohungsabwehr, Deception-Technologien, die Minimierung seitlicher Bewegungen und Bedrohungsinformationen.



Automatisierung ermöglicht eine schnelle Erkennung und Abwehr von Bedrohungen und maximiert die Verfügbarkeit von OT-Systemen.

Die FortiSandbox aktiviert verdächtige Objekte in einer simulierten Umgebung.

Der FortiDeceptor enttarnt Angreifer im Netzwerk mit Decoys – virtuellen Maschinen (VM), die als Köder fungieren und vermeintliche Angriffsziele vorspiegeln.

Maximale Verfügbarkeit von Betriebstechnologie (OT) mit automatisierter Bedrohungsabwehr

OT-Umgebungen haben sehr hohe Verfügbarkeitsanforderungen. Fortinet-Lösungen ermöglichen eine schnelle, unterbrechungsfreie Erkennung und Abwehr von Bedrohungen: Mit einer strategischen Security-Automatisierung werden sofort Gegenmaßnahmen ergriffen, wobei die Kontrolle weiterhin bei Ihrem Team liegt.

Der **FortiAnalyzer** sammelt automatisch Protokolldaten aus dem gesamten OT-Netzwerk. Mit maschinellem Lernen werden die Daten korreliert, um Indikatoren für potenzielle Bedrohungen zu extrahieren. Dieser Kontext erlaubt eine schnelle Reaktion, um die Angriffsfolgen für das Netzwerk zu minimieren.

FortiSIEM übernimmt das Ereignis-Management für das gesamte Unternehmen. Durch die zentrale Übersicht über Alarmdaten in einer einzigen Konsole erhalten Analysten einen vollständigen Überblick über den aktuellen Status der Netzwerk-Infrastruktur. Dies unterstützt eine schnelle Reaktion auf Bedrohungen, die das Netzwerk gefährden.

FortiSOAR bietet eine Security-Orchestrierung, Automatisierung und Bedrohungsabwehr. OT-Betreiber können Prozesse automatisieren, um auf häufig auftretende Sicherheitsvorfälle zu reagieren. Wurde eine Bedrohung erkannt, kann der Analyst

automatisierte Reaktionen ausführen, die das Problem beheben und zugleich die Auswirkungen auf den Betrieb und die Systemverfügbarkeit minimieren.

Die Fortinet Security Fabric ermöglicht die Integration von Fortinet-Lösungen sowie von über 350 Produkten von Drittanbietern. Dank dieser Integration können alle Lösungen aktuelle Bedrohungs- und Telemetriedaten austauschen. Unternehmen profitieren dadurch von einer koordinierten Bedrohungsabwehr im gesamten OT-Netzwerk.

Fortinet bietet auch einen Endpunkt-Schutz, der auf die Hochverfügbarkeits-anforderungen von OT-Umgebungen zugeschnitten ist.

Der **FortiEDR** bekämpft Bedrohungen auf kompromittierten Endpunkten. Infektionen werden auf Prozessebene eingedämmt, statt die betroffenen Prozesse zu beenden. So können infizierte Systeme den Betrieb aufrechterhalten, ohne das restliche Netzwerks zu gefährden. FortiEDR startet zudem automatisierte, auf Playbooks basierende Reaktionen auf häufige Bedrohungen, um die Auswirkungen von Sicherheitsvorfällen zu minimieren. Dank seiner geringen RAM- und CPU-Anforderungen läuft FortiEDR problemlos auf Rechnern mit wenigen Ressourcen und Altsystemen, die auch heute noch in vielen
OT-Netzwerken zu finden sind.

Deception-Technologien gegen hochkomplexe Bedrohungen

Hochkomplexe Cyber-Bedrohungen arbeiten mit ausgefeilten, gezielten Angriffen, um herkömmliche Bedrohungserkennungen zu umgehen. Mit den Deception-Technologien von Fortinet können OT-Unternehmen Angreifer aufspüren, die unbemerkt ins Netzwerk eingedrungen sind.

Die **FortiSandbox** emuliert Systeme, die häufig in OT-Netzwerken zu finden sind, damit verdächtige Objekte in Quarantäne getestet werden können. Dies ermöglicht die Analyse von OT-spezifischer Malware und die Erkennung von Angreifern, die sich bereits im OT-Netzwerk befinden.

FortiDeceptor emuliert OT-Steuerungssysteme, um Angreifer mit diesen „Fake-Systemen“ aus dem Versteck zu locken. Das für Betriebstechnologie zuständige Network-Operations-Team kann so interne Bedrohungen innerhalb des Netzwerks identifizieren und Informationen über die Tools und Vorgehensweisen von Angreifern gewinnen.

Die Segmentierung ist eine grundlegende Best Practice zur Sicherung von Betriebstechnologie (OT), wie in den Sicherheitsstandards ISA/IEC-62443 (früher ISA-99) beschrieben.[1]

Fortinet-Lösungen lassen sich leicht an OT-Netzwerk-Protokolle anpassen und können so anomale oder bösartige Befehle identifizieren, die an Betriebstechnologie gesendet werden.

Fortinet wird regelmäßig im Gartner Magic Quadrant für Netzwerk-Firewalls als Leader eingestuft und hat in der NGFW Security Value Map der NSS Labs die höchste Punktzahl erzielt.

Verhindern seitlicher Bewegungen in OT-Netzwerken

Bedrohungsakteure, die sich quer durch das OT-Netzwerk bewegen, können weitere Systeme und Standorte infizieren, die sich im gleichen Netzwerk befinden. Fortinet-Lösungen unterstützen die interne Netzwerk-Transparenz, Zugriffskontrollen und die Durchsetzung von Richtlinien, um zu verhindern, dass sich Bedrohungen lateral im Netzwerk verbreiten.

FortiGate Next Generation Firewalls (NGFWs) können im OT-Netzwerk eine interne Segmentierung anlegen. Sie nutzen eine Datenbank mit über 50 OT-Protokollen und mehr als 1750 Befehlen, um anomalen oder bösartigen OT-Traffic zu erkennen. So wird verhindert, dass eine Bedrohung von einem Segment im OT-Netzwerk auf das nächste überspringt.

FortiNAC bietet eine Netzwerk-Zugriffskontrolle (Network Access Control) und ist bereits in FortiGate NGFWs integriert. Die Lösung überwacht das Netzwerk kontinuierlich und identifiziert automatisch alle verbundenen Geräte sowie Geräte, die auf das OT-Netzwerk zugreifen wollen. FortiNAC überprüft auch, ob die Geräte die Sicherheitsrichtlinien des Unternehmens erfüllen. Zudem steuern interne virtuelle lokale Netzwerke (VLANs) den Verkehrsfluss innerhalb des Netzwerks und begrenzen die seitliche Ausbreitung von Cyber-Bedrohungen quer im Netzwerk.

Der **FortiAuthenticator** bietet einen zusätzlichen Schutz vor seitlichen Bewegungen von Benutzern und Geräten im Netzwerk. Unternehmen erhalten damit eine Multi-Faktor-Benutzerauthentifizierung und können rollenbasierte Zugriffskontrollen durchsetzen. Das minimiert die Chance, dass ein Angreifer mit gestohlenen Anmeldedaten auf OT-Systeme zugreifen kann. Außerdem wird die Maschine-zu-Maschine-Kommunikation mit Zertifikaten gesichert.

Bessere Erkennung mit Bedrohungsinformationen speziell für Betriebstechnologie

Fortinet investiert kontinuierlich darin, OT-spezifische Protokolle, Befehle, Systeme und Bedrohungen noch besser zu verstehen und zu unterstützen. Bedrohungsinformationen speziell für Betriebstechnologie werden automatisch und in Echtzeit von den **FortiGuard Labs** über die Fortinet Security Fabric direkt an Fortinet-Lösungen gesendet.

Dank der FortiGuard Threat Intelligence können FortiGate NGFWs OT-Systeme virtuell patchen, um sie vor neu entdeckten Schwachstellen zu schützen.

Der **FortiAnalyzer** – die Logging- und Reporting-Lösung von Fortinet – automatisiert die Kontextanalyse anhand der Indicators of Compromise (IOCs), die von den FortiGuard Labs bereitgestellt werden. Diese IOC-Daten liefern Kontextinformationen zur Bedeutung eines Indikators und seinen Folgen für die Netzwerk-Sicherheit – für Teams eine große Entlastung, weniger Fehlalarme gesichtet werden müssen.

Der **FortiTester** bietet automatisierte Tests mit dem MITRE ATT&CK Framework, um das Verhalten eines Cyber-Angreifers nach der Kompromittierung im Unternehmensnetzwerk zu simulieren.

Das **Fortinet Fabric-Ready-Partnerprogramm** ist ein Ecosystem aus Security- und Netzwerk-Partnern, deren Lösungen in die Fortinet Security Fabric integriert sind. Der Informationsaustausch zwischen den FortiGuard Labs und diesen Partnern beschleunigt die Bedrohungserkennung und -abwehr um ein Weiteres.

Verlässliche Bedrohungsinformationen

Die FortiGuard Labs – eine spezielle Fortinet-Einrichtung für Threat Intelligence – gibt es jetzt seit 15 Jahren.
Neben der Identifizierung von IT-Bedrohungen und der Erkennung von Zero-Day-Threats mithilfe künstlicher Intelligenz (KI) und maschinellem Lernen (ML) bieten die FortiGuard Labs auch zuverlässige Bedrohungsdaten speziell für Betriebstechnologie.

Fortinet veröffentlichte den ersten Threat Report der Branche zu Cyber-Sicherheitsbedrohungen und aktuellen Entwicklungen für OT-Umgebungen.

Fazit

Um hochkomplexe Cyber-Bedrohungen effektiv zu bekämpfen, benötigen Network-Operations-Analysten für Betriebstechnologie (OT) eine überschaubare und zugleich tiefengestaffelte Sicherheitsarchitektur. Die Fortinet Security Fabric erfüllt diese Anforderungen mit umfassenden, integrierten und automatisierten Lösungen für OT- und IT-Umgebungen. Diese Lösungen bieten eine Erkennung und Abwehr von hochentwickelten Bedrohungen, zuverlässige Analysen und Berichte sowie eine zentrale Transparenz und Verwaltung – alles über eine einzige Management-Konsole.

Für weitere Informationen wenden Sie sich bitte an info@fortinet.com.

[1] „ISA Standards: Numerical Order“. International Society of Automation, abgerufen am 12. Juni 2020.

FORTINET

www.fortinet.com/de

7. Dezember 2020, 13:59 Uhr

670238-0-1-DE