SOLUTION BRIEF

Einfachere, verlässlichere OT-Security mit FortiNAC

Zusammenfassung

Ob in der Fertigung oder in kritischen Infrastrukturen – die Security von Betriebstechnologie (OT) ist von entscheidender Bedeutung. Steuerungstechnik wie ICS- und SCADA-Systeme gibt es zwar schon seit vielen Jahren, doch eine stärkere Vernetzung und die zunehmend komplexe Bedrohungslage haben ihre Anfälligkeit für Angriffe erhöht. Einer der Bereiche, in denen Fortinet zum Schutz von OT-Umgebungen beiträgt, ist die Netzwerk-Zugangskontrolle (Network Access Control). FortiNAC kann als eigenständige Lösung oder als Teil der größeren Fortinet Security Fabric implementiert werden, um eine übergreifende Transparenz und Kontrolle für OT-Netzwerke zu gewährleisten.

SCADA und ICS kurz erklärt

ICS-Systeme werden häufig über SCADA-Systeme verwaltet. Diese bieten eine grafische Benutzeroberfläche für den Bediener, um den Status eines Systems zu beobachten, Warnungen zu erhalten oder Anpassungen des Prozess-Managements vorzunehmen.

Es wird erwartet, dass der wachsende ICS-Markt 2021 umgerechnet 67,7 Milliarden € erreicht.

Für den SCADA-Markt wird ein jährliches Wachstum von 6,6 % auf ein Marktvolumen von umgerechnet 11,23 € in 2022 prognostiziert.[4]

Höhere Risiken für SCADA und ICS durch Konvergenz

Ursprünglich waren OT-Umgebungen – insbesondere ICS- und SCADA-Systeme – aufgrund ihrer Isolation von öffentlichen Netzwerken und dem Internet sicher und wurden praktisch nie angegriffen. Folglich gab es keinen Grund, Security-Technologien wie speicherprogrammierbare Steuerungen (SPS) zu integrieren. Dies hat sich in den letzten Jahren geändert, als die „Mauer“ zwischen Betriebstechnologie (OT) und Informationstechnologie (IT) fiel. Laut einer aktuellen Umfrage sind in den meisten Unternehmen mittlerweile OT- und IT-Systeme vernetzt. Dadurch steigt jedoch die Gefahr, dass Hacker in diese Steuerungssysteme eindringen.[1]

Nach dem Ausfall des ukrainischen Stromnetzes im Dezember 2015, als ein facettenreicher SCADA-Angriff die Stromversorgung für 80.000 Kunden abschaltete, begriffen Unternehmen schnell, wie anfällig diese Systeme sind.[2] Diese Anfälligkeit besteht weiterhin: Änderungen am Netzwerk – größtenteils durch die digitale Transformation – haben zur Vernetzung vieler SCADA-Systeme mit dem Internet und Clouds geführt. Zudem umfassen OT-Systeme jetzt auch vernetzte Funktionen wie intelligente Umgebungskontrollen (z. B. für die Beleuchtung, Brandbekämpfung oder Raumlufttechnik). Jede dieser neuen Verbindungen „ebnet“ Bedrohungen den Weg in Systeme, bei denen bislang auf eine starke Security verzichtet wurde.

Das Security-Management für OT-Systeme ist eine Herausforderung für sich – insbesondere für Energieversorger, dezentrale Produktionsstandorte und andere Betreiber kritischer Infrastrukturen. Die Anbindung dieser Systeme an das Internet bietet zwar große Vorteile, birgt jedoch auch zahlreiche neue Risiken in sich, mit denen viele OT-Management-Teams wenig Erfahrung haben. Da diese Netzwerke immer komplexer werden und unterschiedlichste Steuerungstechnik, ICS/SCADA-Systeme und SPS verbinden, ist eine zentrale Verwaltung und Security notwendig. Gebraucht wird ein starker „Schutzwall“, damit sich nur bekannte Benutzer und Geräte mit dem OT-Netzwerk verbinden können.

Warum die IoT-Security so schwierig ist

OT-Systeme stellen eine sehr große Angriffsfläche dar. Schon 2017 berichteten in einer Studie von Forrester Consulting fast 60 % der Unternehmen mit SCADA-Anwendungen oder Steuerungstechnik (ICS) von Angriffen auf diese Systeme. Von den Befragten hatten 97 % die Herausforderungen erkannt, die das Zusammenwachsen von IT und OT mit sich bringen.[3]

Aufgrund ihrer bisherigen Isolation werden bei der IT-Cyber-Security weder ICS- noch SCADA-Systeme einbezogen. Erschwerend kommt hinzu, dass viele dieser Altsysteme nicht gepatcht oder aktualisiert werden können. Diese ungesicherten Endpunkte sind deshalb besonders attraktive Angriffsziele: Erstens bieten sie Zugriff auf wertvolle Netzwerk-Daten und zweitens gehören sie oft zur kritischen Infrastruktur eines Landes (z. B. Elektrizität, Öl, Gas, Wasser, Verkehrsnetz).

Durch das zunehmende Zusammenwachsen von IT und OT entstehen Schwachstellen in drei zentralen Bereichen:

1. Mangelnde Transparenz

Fehlt eine umfassende, zentralisierte Transparenz über Geräte, werden OT-Netzwerke anfällig für Angriffe. Die Fülle an vernetzten Geräten – einschließlich IoT-Geräte und geschäftlich genutzte Privatgeräte bei BYOD-Konzepten (Bring your own device) – führt zu unzähligen Endpunkt-Schwachstellen. Dadurch erhöht sich die Anzahl potenzieller Zugriffspunkte für seitliche Angriffe, die sich quer im Netzwerk verbreiten können. Security-Teams müssen deshalb alle Geräte in jedem Standort sehen können, die sich mit dem Netzwerk verbinden wollen – auch am äußersten Netzwerk-Rand.

Immer intelligentere, vernetzte CS-Sensoren, Raumlufttechnik und Steuerungen bringen nicht nur mehr Funktionen, sondern auch neue Einstiegspunkte für Angriffe auf OT-Systeme mit sich. Besonders bei IoT-Geräten fehlen Sicherheitsstandards – wenn überhaupt ein Schutz vorhanden ist. Zudem funktionieren IoT-Geräte ohne zugeordneten Benutzer. Das ist ein Problem für die meisten Firewalls und Security-Lösungen, die den Zugriff über nutzerbasierte Kriterien regeln.

2. Keine Kontrolle

Ein flaches, offenes internes Netzwerk macht es Hackern, böswilligen Benutzern und automatisierter Malware extrem leicht, ungehindert im gesamten Unternehmen nach Geschäftsgeheimnissen zu suchen und interne IP-Adressen in Erfahrung zu bringen. Unternehmen müssen deshalb Zugriffsrichtlinien anwenden und durchsetzen können, die darauf basieren, wer und was mit dem Netzwerk verbunden ist. Dynamische rollenbasierte Netzwerk-Zugangskontrollen erstellen logische Netzwerk-Segmente, die Anwendungen gruppieren, Daten miteinander verknüpfen und den Zugriff auf bestimmte Gruppen beschränken. Dies alles erhöht die Sicherheit des internen Netzwerks.

Die Kontrolle von Benutzern und Geräten ist ein besonders wichtiger Faktor für die Compliance. Viele heutige Industriestandards und Datenschutzgesetze erfordern eine strenge Netzwerk-Zugangskontrolle und Datensicherheit – wie z. B. die Datenschutz-Grundverordnung (DSGVO), der PCI-DSS-Standard (Payment Card Industry Data Security Standard), Sarbanes-Oxley (SOX), das US-Gesetz zur Übertragbarkeit von Krankenversicherungen und zur Rechenschaftspflicht der Krankenversicherer (HIPAA) oder Vorschriften der US-Börsenaufsichtsbehörde SEC (U.S. Securities and Exchange Commission). Bei Nichterfüllung müssen Unternehmen mit Geldstrafen rechnen, die sich pro Datenschutzverletzung auf Millionenbeträge belaufen können.

3. Keine rechtzeitige Lageerkennung

Wird ein einzelnes Gerät angegriffen, müssen die Bedrohungsinformationen automatisch weitergegeben werden. Nur so lässt sich unternehmensweit eine koordinierte Bedrohungsabwehr erreichen. In der Praxis müssen Security-Teams jedoch täglich oft unzählige Alarme sichten und überprüfen. Selbst wenn ein Security-Administrator über verdächtige Aktivitäten an einer bestimmten IP-Adresse informiert wird, kann es Stunden dauern, bis ein verdächtiges Gerät manuell gefunden und alle anderen relevanten Informationen rund um das Ereignis untersucht wurden – nur um zu wissen, ob es sich um einen Angriff, eine Anomalie oder einen Fehlalarm handelt.

Angriffe mit FortiNAC abwehren

Um Sicherheitsprobleme bei Steuerungstechnik, SCADA-Systemen, IoT-Geräten, geschäftlich genutzten Privatgeräten (BYOD) und anderen Endpunkten in den Griff zu bekommen, ist eine erweiterte Netzwerk-Zugangskontrolle als Teil einer umfassenden Security-Architektur erforderlich. Fortinet FortiNAC kann als eigenständiges Produkt oder integriert in die größere Fortinet Security Fabric implementiert werden, um den Netzwerk-Zugriff für ungesicherte Endgeräte zu schützen.

In Abstimmung mit weiteren Fortinet-Lösungen schützt FortiNAC stark dezentrale Netzwerke vor SCADA-Bedrohungen, 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 automatisch wieder ins Netzwerk gebracht werden. Da industrielle Umgebungen zunehmend mit dem Internet verbunden sind, ist FortiNAC eine wichtige Ergänzung zum Schutz ungesicherter ICS- und SCADA-Systeme. Hiermit lässt sich verhindern, dass sich ungenehmigte Elemente mit einem OT-Netzwerk verbinden. FortiNAC bietet drei Hauptfunktionen, die die Netzwerk-Security verbessern: Transparenz, Kontrolle und automatische Benachrichtigungen über Bedrohungen.

1. Vollständige Transparenz über alle Endgeräte

Die bereits erwähnte Forrester-Umfrage ergab, dass 82 % der Unternehmen nicht alle mit ihrem Netzwerk verbundenen Geräte identifizieren können.[5] Da es unmöglich ist, das Netzwerk vor einer Bedrohung zu schützen, die man nicht sehen kann, ist eine lückenlose, unternehmensweite Echtzeit-Transparenz ein entscheidender erster Schritt zur Sicherung von Endgeräten. FortiNAC legt von jeden mit dem Netzwerk verbundenen Endpunkt ein Profil an, einschließlich des physischen Standorts und des Gerätetyps.

2. Einzigartige Kontrolle über ungeschützte Geräte

FortiNAC unterstützt die Verantwortlichen für das SCADA- und ICS-Systemmanagement bei der vollständigen Kontrolle über ihr Netzwerk und kümmert sich um alle neuen Geräte, die sich mit dem Netzwerk verbinden oder mit anderen Infrastrukturbereichen des Unternehmens kommunizieren wollen. Verdächtige Anfragen lassen sich z. B. zurückstellen, bis ein Administrator den Zugriff genehmigt hat.

So können Unternehmen Störungen kritischer Systeme vermeiden. Auch lassen sich mit FortiNAC Kriterien festlegen und Richtlinien durchsetzen, um zu steuern, welche Benutzer auf das Netzwerk zugreifen dürfen und wie viel Zugriff gewährt wird. Hier kann FortiNAC die Konfigurationen ändern, um Segmentierungsrichtlinien für Switche und drahtlose Produkte unterschiedlichster Anbieter zu implementieren. Diese dynamischen Steuerelemente erweitern die Reichweite der Security Fabric in heterogenen Umgebungen. Automatisierte Regeln in FortiNAC lösen Containment-Einstellungen in anderen Security-Fabric-Elementen wie FortiGates, FortiSwitch oder FortiAP aus. Auch Fabric-Ready-Lösungen von Drittanbietern werden unterstützt.

Der Zugriff auf Steuerungsfunktionen erfolgt über ein benutzerfreundliches webbasiertes Management-Dashboard, das sich umfassend anpassen lässt. Potenzielle Bedrohungen werden eingedämmt, indem verdächtige Benutzer oder anfällige Geräte isoliert oder Eindämmungsmaßnahmen durchgesetzt werden. Dies reduziert die Eindämmungszeit von Tagen auf Sekunden, gewährleistet die Einhaltung immer strengerer Branchenvorschriften und schützt kritische Daten und geistiges Eigentum.

3. Automatisierte Bedrohungsmeldungen

Wird ein verdächtiges Ereignis erkannt, sendet FortiNAC automatisierte Bedrohungsmeldungen an das Security Operations Center (SOC). Als Teil der Fortinet Security Fabric lässt sich FortiNAC nahtlos in die umfassendere Sicherheitsarchitektur integrieren. Das verbessert die Genauigkeit von Warnungen: Bedrohungsdaten werden in Echtzeit gesendet und empfangen, um das gesamte Unternehmen koordiniert zu informieren. Diese Art der Automatisierung ist der „heilige Gral“ einer vernetzten Security-Architektur.

Die Orchestrierungsebene von FortiNAC sammelt alle Security-Daten, um Bedrohungen automatisch nach Priorität zu sichten. FortiNAC sendet dann automatisch eine Warnung an das SOC. Diese enthält auch Echtzeit-Informationen zum Kontext eines Vorfalls, damit Security-Analysten Bedrohungen schnell lokalisieren und klären können. Dadurch verkürzt sich die Eindämmungszeit oft von Tagen auf Sekunden. Gleichzeitig wird die Einhaltung immer strikter Vorschriften und Standards unterstützt – Stichwort „Compliance“.

Zugriffskontrolle mit einer flexiblen, skalierbaren Plattform

Neben FortiNAC bietet Fortinet weitere umfassende Sicherheitslösungen für OT-Umgebungen.

Mit den Kernfunktionen des Fortinet-Portfolios erhalten Unternehmen starke Security-Features wie:

- Segmentierung und Schutz für die Kommunikation
- Sichere kabelbasierte und drahtlose Zugänge
- Implementierung einer rollenbasierten Zugriffssteuerung für Benutzer, Geräte, Anwendungen und Protokolle
- Management-Protokolle zum Beheben von Schwachstellen und Installieren von Patches
- Identifizieren und Profilieren von Geräten und Ressourcen
- Identifizieren und Blockieren von Malware und Zero-Day-Bedrohungen

Als Teil der Fortinet Security Fabric bietet FortiNAC eine Plattform für die Security-Automatisierung und -Orchestrierung, die als Hardware-Appliance, virtuelle Appliance oder Cloud-Dienst bereitgestellt werden kann. Security-Architekten erhalten damit eine flexible NAC-Lösung passend für die einzigartigen Anforderungen jeder Netzwerk-Umgebung. FortiNAC lässt sich flexibel skalieren und senkt die Gesamtbetriebskosten (TCO), da nicht an jedem Implementierungsstandort ein Server erforderlich ist. Die Lösung nutzt vorhandene Verzeichnis-, Netzwerk- und Sicherheitsinfrastrukturen, um vorhandene Investitionen zu schützen und Störungen zu minimieren.

Mit einer zentralen Kontrolle und der Möglichkeit, gefährdete Altsysteme über das Netzwerk zu schützen – ohne dass größere Upgrades nötig sind –, bietet FortiNAC eine starke Security-Lösung, die sich ideal zum Schutz zunehmend anfälliger OT-Netzwerke vor unautorisierten Geräten oder Benutzern eignet.

Anwenderbericht: Öl- und Gaskonzern sichert kritische Infrastruktur mit FortiNAC

Kritische Infrastrukturen und Versorgungsunternehmen entwickeln sich infolge von Marktveränderungen ständig weiter. Zugleich müssen ihre Systeme gehärtet werden, damit Angriffe auf regelwidrige Endpunkte die Bereitstellung nicht gefährden. Vollständige Transparenz und Kontrolle über den Netzwerk-Zugriff sowie eine funktionierende Bedrohungsabwehr für alle Systeme sind daher entscheidend. Dies kann jedoch schwierig für Energieversorger mit oft stark dezentralen ICS-Operations sein, da manuelle Wartungen und Updates durch IT-Teams zu aufwendig sind.

Ein führender Öl- und Gaskonzern mit 5000 Endpunkten an 200 Standorten in Nordamerika entschied sich für FortiNAC, um den Netzwerk-Zugriff auf dezentrale End- und Altgeräte zu regeln.

FortiNAC dient nun als Master-Steuerung für dezentrale Standorte. Komplexe Hardware-Installationen oder Upgrades älterer Geräte waren nicht notwendig.

Da die Fortinet-Lösung zentralisiert ist und keine Bandbreiten-Zuweisung erfordert, konnte der Kunde bisherige Bandbreiten-Engpässe ohne Appliance-Installationen an Remote-Standorten erfolgreich lösen. Das Unternehmen verfügt jetzt über netzwerkweite Transparenz mit einer Live-Übersicht über sämtliche bestehenden Verbindungen an allen Standorten – einschließlich dezentraler Remote-Switche, Endgeräte und Benutzer.

Anwenderbericht: Gibson Energy

Gibson Energy ist spezialisiert auf Transport, Lagerung, Beimischung, Verarbeitung und Vertrieb von Rohöl und anderen raffinierten Produkten. Gibson Energy hat seinen Hauptsitz im kanadischen Calgary und bietet auch Dienstleistungen im Bereich Ölfeld-Abfallmanagement und Wassermanagement an.

Als Midstream-Energieunternehmen verfügt Gibson über Tausende Feldgeräte, die bis vor kurzem manuell oder gar nicht verwaltet wurden. Mit neuen IoT-Geräten kamen jedoch Verbindungen zu IT-Netzwerken hinzu. Um die operative Integrität sicherzustellen, war nun mehr Transparenz und Kontrolle über alle Geräte notwendig.

Die Betriebsteams von Gibson haben sich für FortiNAC entschieden, um ungesicherte Geräte über ein anpassbares, webbasiertes Dashboard in Echtzeit per Fernzugriff zu beobachten und zu verwalten. Will ein neues Gerät eine Verbindung herstellen oder mit anderen Teilen seiner Infrastruktur kommunizieren, kann FortiNAC verdächtige Anforderungen zurückstellen, bis ein Administrator den Zugriff genehmigt hat. Seit der Implementierung hat Gibson mit FortiNAC Tausende Arbeitsstunden beim manuellen Geräte-Management eingespart.

„Für die Verwaltung und Kontrolle kritischer Ressourcen benötigten wir detaillierten Zugriff auf Firewalls und andere Security-Tools, um ein einheitliches Sicherheitsprofil zu schaffen und aufrechtzuerhalten. Deshalb haben wir uns für Fortinet entschieden“, erklärt Richard Hannah, Vice President Information Services bei Gibson Energy.

[1] „Independent Study Pinpoints Significant SCADA/ICS Security Risks“. Fortinet, 17. Mai 2018.

[2] „Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid“. Wired, 3. März 2016.

[3] „Independent Study Pinpoints Significant SCADA/ICS Security Risks“. Fortinet, 17. Mai 2018.

[4] „Independent Study Pinpoints Significant SCADA/ICS Security Risks“. Fortinet, 17. Mai 2018.

[5] „IoT Security Fail: 82 Percent of Companies Can’t Identify All Network-Connected Devices“. eSecurity Planet, 8. November 2017

FORTINET

www.fortinet.com/de

14. Dezember 2020, 14:19 Uhr

617953-0-0-DE