WHITEPAPER

Sicherer, skalierbarer Zugang für Betriebstechnologie (OT)

Wie Sie Remote-Arbeitsplätze unterstützen und einen kontinuierlichen Geschäftsbetrieb gewährleisten

Zusammenfassung

Ob Fabriken, öffentlicher Nahverkehr, Energieerzeugung, Stromnetze, Öl- und Gasanlagen oder Versorgungsunternehmen – Betriebstechnologie (OT) sorgt dafür, dass kritische Infrastrukturen funktionieren. Keine Frage: Ein Plan für einen kontinuierlichen Geschäftsbetrieb ist in diesen Bereichen ein Muss.

Fortinet bietet eine integrierte Lösung für den sicheren Fernzugriff, die die Anforderungen von Betriebstechnologie erfüllt: Bei FortiGate Next-Generation-Firewalls (NGFWs) ist die Unterstützung von virtuellen privaten Netzwerken (VPN) bereits integriert, damit sich Remote-Mitarbeiter von jedem Arbeitsort aus sicher mit IT- und OT-Netzwerken des Unternehmens verbinden können. Durch Kombination von FortiClient und FortiToken für den Endpunktschutz, einer Multi-Faktor-Authentifizierung (MFA) und dem Single Sign-On (SSO) mit FortiAuthenticator können Unternehmen Remote-Arbeitsplätze sicher realisieren und den kontinuierlichen Geschäftsbetrieb aufrechterhalten. Zusätzlich lassen sich mit FortiPAM spezielle Sicherheitsfunktionen für privilegierte Benutzer wie Credential Vaulting, Zero-Trust-Access (ZTA), Monitoring und Reporting bereitstellen, die den Zugriff auf die wichtigsten OT-Geräte des Unternehmens wirksam schützen.

Drei von vier OT-Unternehmen erlebten im Vorjahr mindestens einen illegalen Zugriff auf Systeme.[1]

Aufrechterhalten des Betriebs mit Remote-Arbeit

Viele OT-Unternehmen sind für die öffentliche Sicherheit von entscheidender Bedeutung und müssen den Betrieb auch unter schwierigsten Bedingungen und bei Notfällen aufrechterhalten können – ob hohe Krankheitszahlen, Hochwasserkatastrophen, Sturmschäden oder Stromausfälle.

Bei Notfallplänen sollte unbedingt auch der Fall berücksichtigt werden, dass vor Ort kein normaler Betrieb mehr möglich ist. Um einen kontinuierlichen Geschäftsbetrieb auch dann zu gewährleisten, brauchen Mitarbeiter sichere Remote-Arbeitsplätze. Ebenfalls unverzichtbar ist ein geschützter Fernzugriff, damit selbst in Ausnahmesituationen neue Maschinen in Betrieb genommen werden, kritische Patches angewendet sowie Reparaturen und Fehlerbehebungen durchgeführt werden können. Eventuell ist außerdem eine Fernüberwachung und -diagnose notwendig, um entfernte dezentrale Standorte kostengünstig zu betreiben. Die Security ist dabei von entscheidender Bedeutung. Schließlich können Sicherheitsvorfälle in OT-Umgebungen zu Ausfällen führen können, die Leib und Leben oder kritische Infrastrukturen gefährden.

Fortinet-Lösungen lassen sich problemlos an Remote-Arbeitsplätzen bereitstellen. Viele Unternehmen benötigen jedoch auch Ressourcen vor Ort oder in der Cloud, um Remote-Mitarbeiter sicher zu unterstützen. Oftmals verfügen Unternehmen bereits über diese Ressourcen in ihrer vorhandenen Sicherheitsinfrastruktur und müssen sie nur aktivieren. Entscheidend ist, dass ein Unternehmen bei einer Naturkatastrophe oder anderen Störungen des normalen Geschäftsbetriebs handlungsfähig bleibt und notfalls schnell die gesamte Belegschaft auf Remote-Arbeit umstellen kann. Fortinet-Lösungen sind dafür ideal und sorgen zugleich für eine höhere Sicherheit als ein virtuelles privates Netzwerk (VPN), das lediglich Daten während der Übertragung verschlüsselt.

Mit Fortinet erhalten Unternehmen zahlreiche Security-Funktionen für den Schutz von hybriden Belegschaften und Infrastrukturen, wie z. B.:

- **MFA und SSO:** FortiToken und FortiAuthenticator ermöglichen eine Zwei-Faktor-Authentifizierung und den Single Sign-On (SSO) für Remote-Mitarbeiter und externe Dritte.
- **NGFW, Intrusion Prevention System (IPS), Antivirus, Web-Filter und SD-WAN (Software-Defined Wide-Area Networking):** FortiGate bietet all diese Funktionen und mehr in einer einzigen Appliance.
- **Zugang über Mobilfunknetze:** FortiAP und FortiExtender stellen für Remote-Mitarbeiter einen sicheren, vollintegrierten Zugang über Mobilfunknetze (3G/4G LTE und 5G) bereit, der sich zentral konfigurieren und verwalten lässt.
- **Zugriff für privilegierte Benutzer:** FortiPAM bietet Sicherheitsfunktionen wie Credential Vaulting zum Schutz von Anmeldedaten, Passwortänderungen, Zero Trust, Posture Checking zur Risikoprofil-Bewertung sowie eine Überwachung des Zugriffs auf kritische OT-Systeme durch privilegierte Benutzer.

Als Next-Generation-Firewall kann eine FortiGate NGFW den gesamten verschlüsselten und Klartext-Datenverkehr eines Unternehmens bei minimalen Leistungseinbußen überprüfen. Außerdem bieten FortiGate NGFWs ein integriertes VPN-Gateway, das als Endpunkt für verschlüsselte Verbindungen zu Remote-Mitarbeitern fungiert. FortiGate NGFWs mit dem Betriebssystem FortiOS 7.0 verfügen zudem über einen integrierten Zero-Trust-Network-Access (ZTNA), womit sich der Zugriff auf Anwendungen unabhängig vom Standort des Benutzers oder der Anwendung regeln lässt. Ein ZTNA ist die logische Weiterentwicklung des VPN-Fernzugriffs. Da er eine höhere Sicherheit, engmaschigere Kontrolle und bessere Nutzererfahrung gewährleistet, ist ein ZTNA ideal für sichere Remote-Verbindungen und Remote-Arbeitsplätze.

FortiGate NGFWs und FortiAP Wireless Access Points lassen sich mit Zero-Touch-Provisioning bereitstellen. Die Vorkonfiguration ist vor dem Versand möglich, damit die Lösungen vor Ort automatisch installiert werden können.

Eine FortiGate NGFW lässt sich in weitverbreitete IT-Infrastrukturelemente integrieren, z. B. in unternehmenseigene Verzeichnisdienste wie Microsoft Active Directory (AD) oder MFA- und SSO-Lösungen. Der FortiAuthenticator dient dabei als zentraler Integrationspunkt für Authentifizierungslösungen. Er funktioniert mit Drittlösungen sowie mit FortiToken (als Hardware-, Software- oder E-Mail-basierte Option erhältlich). Die Software-Token unterstützen zahlreiche Smartphones und andere Mobilgeräte.

FortiGate VM kann als virtuelle Appliance mit 20 Gbit/s auf AWS und anderen Cloud-Diensten mit großen Instanzen ausgeführt werden. Damit lassen sich Tausende von Remote-Benutzern unterstützen – unabhängig davon, ob sie FortiClient oder VPN-Clients von Drittanbietern verwenden. In vielen Umgebungen werden FortiGate VMs für sichere Verbindungen zu cloudbasierten Security-Services-Hubs eingesetzt. Der Vorteil ist, dass hiermit sowohl sicher auf Cloud-Anwendungen als auch auf On-Premises-Anwendungen über die nächstgelegene Cloud-Region und private Rechenzentren zugegriffen werden kann. Unternehmen erhalten so eine kontinuierliche Unterstützung für Hochgeschwindigkeits-Datenübertragungen zwischen Clouds und Rechenzentren.

FortiGate NGFWs: Sicherheit für Remote-Arbeitsplätze

Die leistungsstarken IPsec- und SSL-VPNs sowie der ZTNA (bei allen FortiGate NGFWs bereits integriert) bieten IT- und OT-Unternehmen ein flexibles Bereitstellungsmodell. Bei Arbeitsmodellen wie Work-from-Anywhere (WFA) können Remote-Mitarbeiter den ZTNA oder das VPN ohne oder mit einem Client verwenden. Letztere Option bietet zusätzliche Funktionen und wird über den FortiClient-Endpunktschutz implementiert. Noch mehr Wireless-Funktionen für eigene Mitarbeiter oder auch externe Nutzer lassen sich mit einem FortiAP Wireless Access Point oder FortiExtender Wireless WAN Extender in Kombination mit einer FortiGate NGFW bereitstellen.

Fortinet-Lösungen sind so konzipiert, dass sie vom ersten Kauf bis zum Ende ihrer Lebensdauer einfach zu verwenden sind. Sowohl FortiGate NGFWs als auch FortiAPs bieten ein Zero-Touch-Provisioning. Damit lassen sich Appliances für Remote-Standorte vor der Auslieferung vorkonfigurieren, um am Einsatzort automatisch in Betrieb genommen zu werden. Diese Zero-Touch-Bereitstellung ist für einen kontinuierlichen Geschäftsbetrieb und die Unterstützung von Remote-Arbeit wichtig, da niemand vor Ort zusätzliche Konfigurationen vornehmen muss – außer das Gerät und die Netzwerkkabel anzuschließen. FortiGate NGFWs sind als physische und virtuelle Appliances erhältlich, wobei die virtuellen FortiGate-Appliances in Public und Private Clouds gehostet werden können.

Da die Fortinet Security Fabric „OT-aware“ ist, erhält Betriebstechnologie den gleichen starken Schutz wie man ihn aus dem IT-Bereich kennt. Die Grundlage dafür bilden FortiOS – Fortinets Netzwerkbetriebssystem – und eine offene API-Umgebung (Application Programming Interface), die gemeinsam eine umfassende, integrierte und automatisierte Sicherheitsarchitektur schaffen. Dank dieser OT-Awareness der Fortinet Security Fabric können alle Geräte eines Unternehmens – einschließlich der Geräte, die bei hybriden Arbeitsmodellen an Remote-Arbeitsplätzen bereitgestellt werden – zentral überwacht und verwaltet werden. Security-Teams erhalten damit volle Transparenz und Kontrolle über sämtliche verbundenen Geräte. Dabei spielt es keine Rolle, wo und worüber die Geräte vernetzt sind – ob lokal über eine FortiGate NGFW oder über eine integrierte, zentrale FortiManager-Plattform in der Unternehmenszentrale.

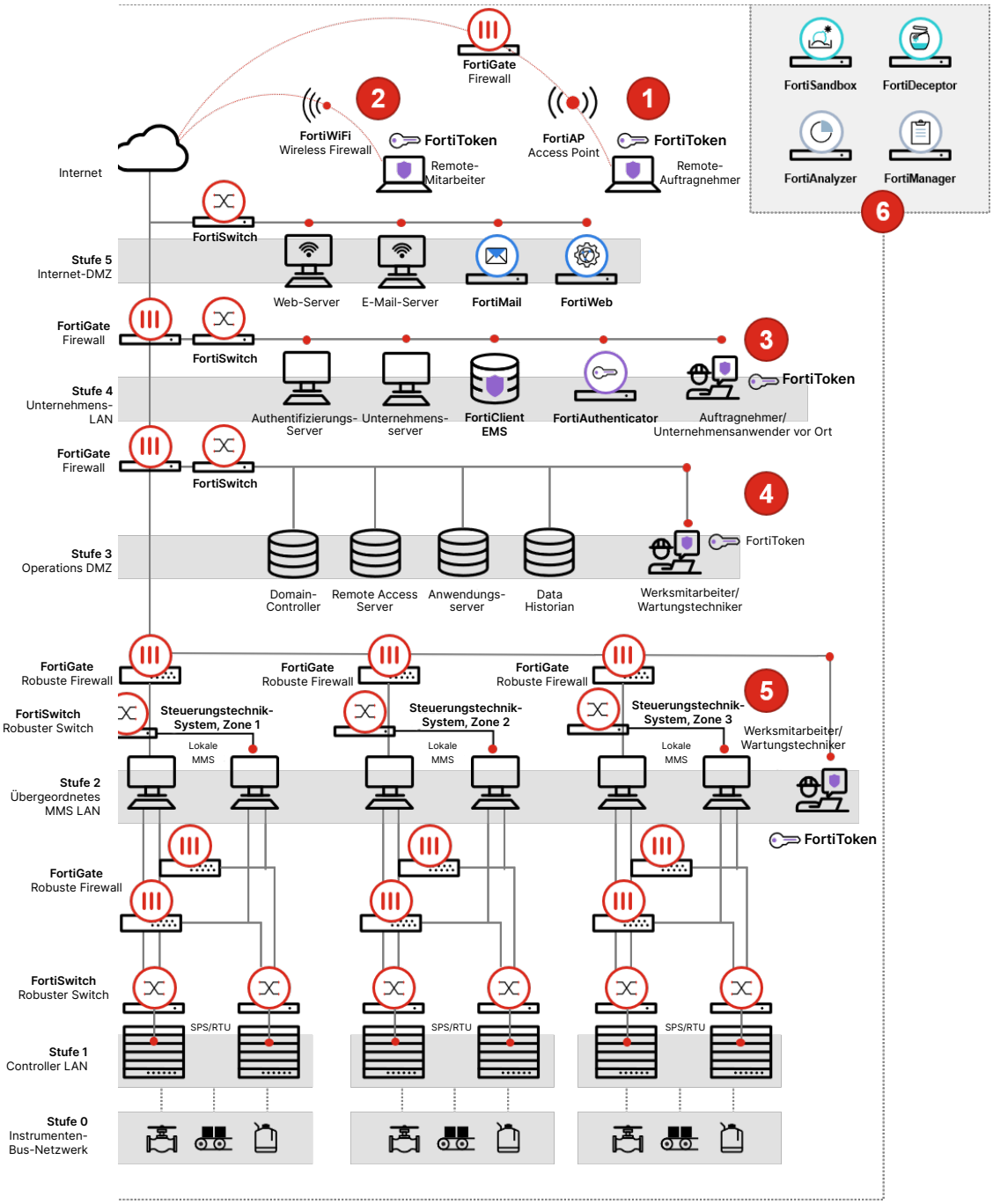

Abbildung 1: Sicherer Zugang mit Fortinet-Lösungen über eine vernetzte IT- und OT-Infrastruktur

Anwendungsfälle für Fortinet-Produkte, die einen sicheren Zugang unterstützen

Bei flexiblen Arbeitsmodellen wie Work-from-Anywhere (WFA) braucht nicht jeder Remote-Mitarbeiter den gleichen Zugriff auf Unternehmensressourcen. Und nicht jedem externen Auftragnehmer oder Lieferanten sollte der Zugang zu kritischen internen Systemen und Netzwerken ohne formelle Autorisierung der Fernzugriffsanforderung und Überwachung von Fernverbindungen gewährt werden. Fortinet bietet deshalb maßgeschneiderte Lösungen für verschiedene Arten von Remote-Anwendern:

1 Sicherer Zugang für Mitarbeiter von Dritten, z. B. zur Fernwartung, Überwachung oder Diagnose (FortiClient, FortiToken, FortiAP, FortiGate, FortiPAM)

Remote-Anwender von Drittfirmen sind oft externe Wartungstechniker, die Industrieanlagen betreuen. Manchmal benötigen diese einen umfassenderen Fernzugriff für die Fehlerbehebung oder den Betrieb von Steuerungstechnik (ICS) in entfernten Standorten. Beispielsweise kann in OT-Umgebungen der Zugriff auf speicherprogrammierbare Steuerungen (SPS) und Fernbedienungsterminals (RTU, Remote-Terminal Units) notwendig sein. Eventuell müssen externe Partner auch in mehreren IT-Umgebungen gleichzeitig arbeiten können. Systemintegratoren, OEM-Lieferanten, Zulieferer und andere Betreiber können ebenfalls zu diesen Drittanwendern gehören, die einen Remote Access brauchen.

2 Sicherer Zugang für Remote-Mitarbeiter, z. B. bei WFA-Arbeitsmodellen wie Telearbeit, Homeoffice oder Hybrid-Working (FortiClient, FortiToken, FortiWiFi, FortiPAM)

Remote-Mitarbeiter benötigen für ihre tägliche Arbeit einen Fernzugriff auf Unternehmenssysteme für E-Mails, Internetnutzung, Videokonferenzen, File Sharing oder Finanz- und Personalfunktionen, um nur einiges zu nennen. In Unternehmen mit Betriebstechnologie brauchen einige Mitarbeiter womöglich zudem Zugriff auf OT-Systeme, um Aufzeichnungen, Protokolle und Daten abzurufen oder Wartungsarbeiten und Diagnosen durchzuführen. Mitarbeiter, die für die Wartung der OT-Infrastruktur verantwortlich sind, müssen z. B. aus der Ferne die Anlagenleistung und Ausfallsicherheit überwachen und bei Problemen Fehler beheben können.

WFA-Mitarbeiter können sich über die integrierte VPN-Client-Software FortiClient oder per ZTNA sowohl mit OT-Systemen als auch mit internen IT-Diensten verbinden und ihre Identität mit FortiToken für die Multi-Faktor-Authentifizierung (MFA) nachweisen.

3 Sicherer Zugang für Auftragnehmer vor Ort oder Unternehmensanwender, die von IT-Netzwerken auf Betriebstechnologie zugreifen müssen (FortiClient, FortiToken, FortiGate, FortiClient EMS, FortiAuthenticator, FortiPAM)

Ähnlich wie bei den ersten beiden Anwendungsfällen (Punkt 1 und 2 oben) müssen Auftragnehmer und Unternehmensanwender vor Ort eventuell vom IT-Netzwerk auf OT-Systeme zugreifen können, z. B. zur Datenabfrage oder bei Wartungsarbeiten. OT-Systeme gehören oft zu dezentralen OT-Netzwerken, die geografisch über viele Standorte verteilt sind. Manchmal befinden sich OT-Netzwerke auch in abgelegenen Gegenden, die schwer erreichbar sind oder wegen der Umgebungsbedingungen keine Arbeiten vor Ort erlauben.

Das IT-Unternehmensnetzwerk kann sich an einem zentralen Standort befinden und mit den OT-Netzwerken an verschiedenen Standorten vernetzt sein. In solchen Fällen ist ein sicherer Fernzugriff auf OT-Netzwerke und OT-Systeme für Auftragnehmer vor Ort oder Unternehmensanwender über das zentrale IT-Unternehmensnetzwerk möglich. Auch lassen sich so zentral Technologien für das Remote-Access-Management implementieren und bereitstellen, wie z. B. eine zentralisierte Autorisierung und Überwachung von Fernzugriffen.

Zur Einhaltung behördlicher Vorschriften ist eventuell für Audits und Compliance-Zwecke ein sicherer Zugang vom IT-Unternehmensnetzwerk auf die OT-Netzwerke nötig. Mitarbeiter im Unternehmen brauchen womöglich auch Zugriff auf OT-Netzwerke, um benötigte Informationen aus der OT-Infrastruktur für CERT-Teams oder Berichte für Behörden wie die ENISA oder das CSIRT zur Erfüllung der NIS-Richtlinie abzurufen. (Auf das zentrale Reporting und Management geht der Anwendungsfall Nr. 6 unten näher ein.)

4 Sicherer Zugang für Werksmitarbeiter und Wartungstechniker, die aus OT-Netzwerken auf Steuerungstechnik zugreifen müssen (FortiClient, FortiToken, FortiGate, FortiPAM)

In Leitstellen oder Kontrollräumen müssen Werksmitarbeiter und Wartungstechniker möglicherweise für betriebliche Routine-Abläufe (wie Überwachung, Diagnose und Wartung) auf Steuerungstechnik (ICS) zugreifen. Die ICS-Leitstelle kann sich vor Ort oder an einem entfernten Standort befinden und per Kabel, WLAN oder WAN verbunden sein.

Zugang und Kommunikation von Leitstellen und ICS-Standorten müssen unbedingt geschützt werden, um Angriffe über das Netzwerk wie Man-in-the-Middle und Lauschangriffe zu verhindern. Zum stärkeren Schutz dieser Zugänge und Netzwerke sollten bei der Bereitstellung eines sicheren Fernzugriffs gleich weitere Security-Funktionen wie eine Multi-Faktor-Authentifizierung (MFA) und die Verschlüsselung von Netzwerkverbindungen implementiert werden. Netzwerktechnologien wie ein SD-WAN sind ebenfalls sinnvoll, wenn Leitstelle und ICS-Standorte über mehrere Kommunikationsverbindungen vernetzt sind und diese zu vertretbaren Kosten ständig verfügbar sein sollen.

5 Sicherer Zugang für Werksmitarbeiter und Wartungstechniker, die vor Ort auf Steuerungstechnik zugreifen müssen (FortiClient, FortiToken, FortiGate, FortiPAM)

Der sichere Zugriff auf Steuerungstechnik muss nicht immer von einem Remote-Standort erfolgen. Aus Sicherheitsgründen müssen Werksmitarbeiter oder Techniker manchmal auch vor Ort auf Steuerungstechnik zugreifen und brauchen dafür einen sicheren Zugang, der mit einer Multi-Faktor-Authentifizierung (MFA) und AAA-Funktionen (Authentifizierung, Autorisierung und Accounting) zusätzlich geschützt wird. Eventuell ist es auch ratsam, innerhalb von ICS-Netzwerken eine Netzwerkverschlüsselung zu implementieren.

Müssen sehr viele sichere Zugänge bereitgestellt werden, können zentralisierte Management-Funktionen den Verwaltungs- und Wartungsaufwand für mehrere Technologien erheblich reduzieren, z. B. beim Aktualisieren einer Software oder Firmware für verschiedene Technologien.

6 Zentralisierte Sicherheitsanalysen, Berichte und Verwaltung mit zentralem, erweiterten Bedrohungsschutz (FortiAnalyzer, FortiManager, FortiSandbox, FortiDeceptor)

Unabhängig davon, ob ein sicherer Zugang vor Ort oder per Fernzugriff vorgesehen ist, sollte unbedingt auch eine zentrale Protokollierung, Überwachung, Berichterstattung und Verwaltung implementiert werden. Nur so lassen sich aussagekräftige Informationen gewinnen und die Secure-Access-Infrastruktur effizient verwalten. Diese zentrale Implementierung von Protokollierung, Überwachung und Berichterstellung kann mit einem Network Operations Center (NOC) oder Security Operations Center (SOC) realisiert werden.

In einigen Fällen kann eine zentralisierte Berichterstattung für interne Compliance-Zwecke an die Unternehmensleitung oder interne Security-Teams notwendig sein. Manchmal sind diese Informationen zur Einhaltung behördlicher Vorschriften wichtig, wenn der Anlagenbetreiber oder -eigentümer staatliche Stellen über Sicherheitsmaßnahmen informieren muss.

Müssen sehr viele sichere Zugänge bereitgestellt werden, können zentralisierte Management-Funktionen den Verwaltungs- und Wartungsaufwand für mehrere Technologien erheblich reduzieren, z. B. beim Aktualisieren einer Software oder Firmware für diverse Technologien.

Um mit neuen Bedrohungen Schritt zu halten, können außerdem fortschrittliche Technologien für den Bedrohungsschutz zentral implementiert werden. Als Advanced Threat Protection empfehlen sich z. B. Sandboxing-Tools wie FortiSandbox, Honeypots oder FortiDeceptor. So lassen sich interne und externe Bedrohungen gut erkennen und Risiken minimieren.

Vollständig integrierte Security mit Fortinet-Lösungen

Beim Management einer auswärts arbeitenden, geografisch verteilten Belegschaft ist eine zentralisierte Security-Transparenz und -Verwaltung unerlässlich. Alle Fortinet-Lösungen können über die Fortinet Security Fabric integriert werden. Unternehmen erhalten damit eine einheitliche Plattform für die Konfiguration und Überwachung mit maximaler Transparenz. Fabric-Konnektoren, eine offene API-Umgebung, die Unterstützung der DevOps-Community und das große erweiterte Ökosystem der Security Fabric ermöglichen zudem die Integration mit über 500 Drittlösungen.

Will ein Unternehmen mit einem Notfallplan den kontinuierlichen Geschäftsbetrieb sicherstellen, sind Transparenz und Management der gesamten Security-Architektur des Unternehmens von entscheidender Bedeutung. Denn möglicherweise wird das Unternehmen gezwungen sein, ohne oder mit geringer Vorlaufzeit vollständig auf Telearbeit und Homeoffices umzustellen – und die Unterstützung von Remote-Arbeit sollte die Cybersecurity eines Unternehmens auf keinen Fall gefährden

Die folgenden Lösungen sind Teil der Fortinet Security Fabric und eignen sich ideal für Remote-Arbeitsplätze und den Fernbetrieb von Betriebstechnologie:

FortiClient unterstützt Endpunkt-Telemetrie, Schwachstellen-Management, Malware-Prävention, Web-Filter, Application Firewalls, VPN-Clients, ZTNA und MFA.

FortiClient EMS ist ein Security-Fabric-Konnektor für die zentralisierte Client-Bereitstellung und -verwaltung und bietet VPN-Client-Konfigurationen sowie Sicherheitsrichtlinien und eine Profilverwaltung für Endpunkte.

FortiAP sorgt für sichere Verbindungen mit drahtlosen Controllern und erweitert Netzwerke für Remote-Anwender mit Zero-Touch-Bereitstellung. Software-VPN-Clients werden damit überflüssig.

FortiExtender bietet hybride WAN-LAN-Konnektivität, flexible drahtlose WAN-Konnektivität und unterstützt unterschiedlichste Mobilfunknetze (3G, 4G LTE und 5G). Ideal für mobile Standorte, Fuhrparks und Außendienst-Teams.

FortiWiFi und **FortiGate** sind sichere drahtlose Controller mit VPN- und ZTNA-Diensten für die Durchsetzung und Zugangskontrolle mit NGFW-Funktionen (Next-Generation Firewall), NGIPS (Next-Generation Intrusion Prevention) und Security-Fabric-Konnektoren. Ideal für dynamische Sicherheitsrichtlinien, SD-WAN und Zero-Touch-Bereitstellung.

FortiToken bestätigt die Identität von Benutzern mit Hardware- und Software-Authentifizierungstoken. Lässt sich nahtlos mit FortiGates und/oder dem FortiAuthenticator integrieren und bietet Software-Tokens für iOS und Android. Ideal für eine sichere Online-Aktivierung mit den KI-gestützten FortiGuard Security Services.

FortiAuthenticator bietet ein Authentifizierungs-Management mit LDAP-, RADIUS- und SAML-Integration, einem MFA- und Token-Management mit Unterstützung von Hardware- und Software-Token sowie Zertifizierungsstellen.

FortiPAM ermöglicht die Verwaltung, Kontrolle und Überwachung von höherrangigen und privilegierten Benutzerkonten, Prozessen und kritischen Systemen in der gesamten OT-Umgebung.

FortiAnalyzer zentralisiert die Protokollierung, Berichterstattung, die Asset- und Netzwerkvisualisierung sowie das Event- und Incident-Management und ermöglicht NOC/SOC-Analysen von implementierten Hardware-Appliances und virtuellen Maschinen (VM).

FortiManager bietet eine zentralisierte Verwaltung und Überwachung, Sicherheitsautomatisierung und unternehmenstaugliche Integration. Unterstützt eine rollenbasierte Administration, Secure SD-WANs, Hardware-Appliances und virtuelle Maschinen (VM).

FortiSandbox bietet eine KI-gestützte Malware-Erkennung und -Reaktion sowie einen automatisierten Schutz vor Sicherheitsverletzungen mit Analysen nach dem MITRE ATT&CK-Framework. Lässt sich nahtlos mit FortiGates und der Fortinet Security Fabric integrieren. Unterstützt ICS/OT-Anwendungen und -Protokolle, zentrale und Einzelbereitstellungen sowie Hardware-Appliances und virtuelle Maschinen (VM).

FortiDeceptor verwendet Decoys und Köder, um Cyberbedrohungen frühzeitig zu beseitigen. Emuliert die Fernsteuerung über Windows, Linux, VPN und ICS-RTUs und lässt sich nahtlos mit FortiGates und der Fortinet Security Fabric integrieren. Unterstützt ICS/OT-Anwendungen und -Protokolle, zentrale und Einzelbereitstellungen sowie Hardware-Appliances und virtuelle Maschinen (VM).

Eine sichere Grundlage für einen kontinuierlichen Geschäftsbetrieb

Sowohl für OT- als auch für IT-Unternehmen ist die Vorbereitung für einen kontinuierlichen Geschäftsbetrieb und die Wiederherstellung nach Sicherheitsvorfällen – Stichwort „Disaster Recovery" – von entscheidender Bedeutung. Bei der Entwicklung eines Notfallplans müssen Unternehmen sicherstellen, dass sie über die richtigen Ressourcen verfügen, um Remote-Mitarbeiter zu schützen. Zudem muss ein unterbrechungsfreier Betrieb der OT- und IT-Infrastruktur sowohl vor Ort als auch per Fernzugriff möglich sein, ohne die unternehmensweite Sicherheit zu gefährden. Das Sicherheitsprofil des Unternehmens sollte ebenfalls jederzeit aufrechterhalten werden.

Fortinet-Lösungen sind dafür ideal geeignet. Sie sind einfach bereitzustellen und zu konfigurieren, damit OT- und IT-Unternehmen – unabhängig von der Implementierungsumgebung – eine durchgängige Sicherheit, Transparenz und Kontrolle für digitale Assets gewährleisten können.

[1] „Bericht zum Stand der Betriebstechnologie (OT) und der Cybersecurity 2023". Fortinet, 24. Mai 2023.

FORTINET

www.fortinet.com/de

30. November 2023

950814-A-0-DE