WHITEPAPER

Fortinet Cybersecurity-Lösungen für die Fertigung

Wie sich IT- und OT-Ressourcen in der Fertigung mit einer einzigen Plattform vor komplexen Bedrohungen schützen lassen

Zusammenfassung

Fertigungsunternehmen betreiben in Werken teure, hochkomplexe Produktionsanlagen mit Steuerungssystemen, die immer häufiger mit dem Internet verbunden werden. Die Folgen dieser Entwicklung für die Cybersecurity sind erheblich – von potenziellen Sicherheitsrisiken im Werk bis hin zu Gefahren für die nationale Sicherheit. Unternehmen wollen deshalb diese Systeme optimal schützen und zugleich Geschäftsanforderungen wie Betriebseffizienz, Produktintegrität und Compliance-Vorschriften erfüllen sowie einen kontinuierlichen Geschäftsbetrieb gewährleisten.
Die Fortinet Security Fabric bietet eine umfassende, integrierte und automatisierte Sicherheitsarchitektur, mit der sich all das erreichen lässt. Unternehmen erhalten damit einen strukturellen Komplettschutz für alle Aspekte des Fertigungsgeschäfts: vom Backoffice bis hin zu Produktionsstandorten, Air-Gap-Systemen,vernetzten Anlagen sowie für interne Benutzer und externe Partner.

Die Häufigkeit und Verbreitung von Exploits sind im Vorjahr bei fast allen ICS/SCADA-Anbietern gestiegen.[4]

Der Fertigungssektor ist von einer zunehmenden Konvergenz geprägt. Während Hersteller früher Produkte im Alleingang produzierten, werden heute Teilprozesse an Partner-Netzwerke outgesourct.[1] Bislang durch das Air Gap geschützte elektronische Systeme sind mittlerweile oft mit IT-Systemen verbunden – und damit mit dem Internet. Kritische Betriebstechnologie (OT), zu der auch Steuerungstechnik (ICS) und SCADA-Systeme (Supervisory Control and Data Acquisition) gehören, wird dadurch einer immer komplexeren Bedrohungslage ausgesetzt und gerät ins Visier von Hackern, die Ziele wie Terrorismus, Cyber-Kriegsführung und Spionage verfolgen.

Durch den globalen Abbau des Air Gaps – dem schützenden „Luftspalt" zwischen Betriebstechnologie und dem Rest der Welt – werden OT-Systeme nun häufiger mit längst bekannten IT-Bedrohungen und speziell entwickelten OT-Exploits angegriffen.[2] Bei einer Umfrage berichteten 74 % der OT-Experten in den letzten 12 Monaten von einem Sicherheitsvorfall.[3] Angriffe auf die kritische Infrastruktur des Fertigungssektors können zu finanziellen Verlusten, Reputationsschäden und manchmal sogar zur Bedrohung der nationalen Sicherheit führen.

Fortinet bietet bereits seit dem Jahr 2005 spezielle Sicherheitslösungen für OT-Umgebungen in kritischen Infrastruktur-sektoren wie Energie, Verteidigung, Fertigung, Lebensmittel und Transportwesen. Durch die maßgeschneiderte Abstimmung der Cyber-Sicherheit auf diese komplexen Infrastrukturen über die Fortinet Security Fabric können Unternehmen die Cybersecurity in OT- und IT-Umgebungen integrieren – von Produktionsstätten bis hin zum Rechenzentrum und mehreren Clouds.

Zentrale Herausforderungen für die Cybersecurity in der Fertigung

Sicherheit für Anlagen, Mitarbeiter, Umwelt und Gesellschaft

In Produktionsstätten gibt es Anlagen, die bei Fehlfunktionen oder einem nicht ordnungsgemäßen Betrieb eine Gefahr für Leib und Leben darstellen können. Dazu kommt, dass sich die aktuelle Bedrohungslage verschärft: Ein cyberphysischer Angriff – die Kombination aus einer Cyber-Attacke und einem Angriff vor Ort auf Anlagen – kann nicht nur Mitarbeiter, sondern auch Anwohner und Menschen in der Nähe gefährden.[5] Darüber hinaus können Angriffe die Sicherheit der hergestellten Produkte beeinträchtigen und sogar ein Risiko für einen größeren geografischen Umkreis bedeuten.

Die meisten Fertigungsunternehmen haben isolierte Systeme für die IT-, OT- und physische Sicherheit, was ein großer Nachteil ist: Allein die IT-Security-Infrastruktur zwischen dem Rechenzentrum, mehreren Clouds und dem Netzwerk-Rand ist oft schon schwierig genug. Aber in Zeiten, in denen Angreifer abgestimmte Cyber-Attacken und physische Angriffe zeitgleich durchführen können, lassen sich Menschenleben oft nur durch das Ineinandergreifen aller Security-Komponenten und mit umfassender, zentraler Transparenz schützen.

Produktivität und Ausfallsicherheit von Anlagen

Jede ungeplante Betriebsunterbrechung kann einen Hersteller viel Geld kosten. Ausfälle können zu Problemen führen, die sich über Vertriebskanäle bis zur Lieferkette auswirken. Viele Cyber-Angreifer wollen Betriebsabläufe stören, andere wollen erst einmal in das Netzwerk eindringen und dann irgendwann zuschlagen. Beides kann den Betrieb empfindlich treffen.

Weil OT-Systeme früher durch ein Air Gap geschützt wurden und auch jetzt noch selten mit Updates aktualisiert werden, ist ihre Cyber-Sicherheit oft schwächer als bei IT-Systemen. Das lockt Cyber-Kriminelle an, die relativ leicht in OT-Systeme eindringen können.[6] Aber selbst wenn Betriebstechnologie weiterhin durch ein Air Gap isoliert ist, kann sie durch Software-Updates kompromittiert werden, die bereits vor der Installation infiziert wurden.

Operative Effizienz

Isolierte Security Operations – aufgrund der mangelnden Integration verschiedener Sicherheitstools – verschlimmern betriebliche Ineffizienzen. Hochbezahlte Cybersecurity-Experten verschwenden dann ihre Zeit mit manuellen Aufgaben wie der Korrelation von Protokollberichten aus verschiedenen Systemen oder dem Zusammenstellen von Compliance-Berichten. Für sinnvolle strategische Sicherheitskonzepte fehlt jedoch die Zeit.

Architektonische Insellösungen schaffen zudem Redundanzen beim Anwendungsmanagement und verlangen von ohnehin schon überlasteten Cybersecurity-Teams spezielle Kenntnisse über jedes Einzelprodukt. Dazu kommen steigende Kosten für Software- und Hardware-Lizenzen – und der damit verbundene Mehraufwand für Mitarbeiter bei der Verwaltung der diversen Lizenzen. All diese Faktoren können die Gesamtbetriebskosten erheblich erhöhen.

Kundenerfahrung

Unabhängig davon, ob Produkte für Endkunden oder Unternehmen gefertigt werden – Hersteller stehen heutzutage immer häufiger in direktem Kundenkontakt und interagieren über soziale Medien, die Unternehmens-Website und andere Customer-Engagement-Tools. Diese Kundennähe kann jedoch von Cyber-Kriminellen ausgenutzt werden, die soziale Netzwerke aus finanziellen Gründen manipulieren. Laut einer Studie werden über die Hälfte der weltweiten Social-Media-Konten von Betrügern betrieben.[7]

Der Schutz von Websites und Social-Media-Interaktionen ist für Hersteller von größter Bedeutung. Schließlich können Verluste der Daten von potenziellen Kunden in Frühphasen des Kaufprozesses den Ruf des Unternehmens dauerhaft schädigen. Auch andere Faktoren können die Kundenerfahrung beeinträchtigen, wie z. B. nicht erreichbare Websites oder Produktengpässe aufgrund von Fertigungsausfällen.

Produktintegrität

Eine – wenn auch nur vorübergehende – Verschlechterung der Produktqualität kann für das Marken-Image katastrophal sein. Wird z. B. durch einen Cyberangriff auf ein OT-System in der Lebensmittelverarbeitung die Temperatur oder die Erhitzungsdauer nur leicht verändert, können Lebensmittel verderben oder an Qualität verlieren. Je nach Produkt können solche Modifikationen sogar Folgen für die Gesundheit und Sicherheit der Verbraucher haben.

Compliance

Abhängig von den gefertigten Produkten unterliegen Hersteller zahlreichen Rechtsvorschriften, Regulierungen und Normen. Die Strafen bei Nichterfüllung können drastisch sein. Noch höhere Kosten entstehen jedoch oft durch Rufschädigungen infolge von Datenpannen.[8]

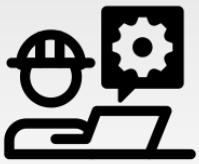
Unternehmen müssen die Einhaltung zahlreicher Vorschriften und Standards nachweisen können, ohne Mitarbeiter zur Vorbereitung von Audit-Berichten von strategischen Initiativen abzuziehen. Nicht nur, dass sich qualifizierte Fachkräfte besser einsetzen lassen als für Audit-Vorbereitungen – diese zeitaufwendige Methode ist auch fehleranfällig: Besteht nämlich die Cybersecurity-Infrastruktur aus vielen isolierten Einzelprodukten, müssen die Daten für Audit-Berichte fast immer manuell abgeglichen werden.

„Seit Jahren wird vor cyberphysischen Angriffen als ernste Bedrohung gewarnt. Aber in den letzten Jahren ist aus dieser potenziellen Gefahr fast unbemerkt eine sehr reale geworden.“[9]

53 % der bestehenden Social-Media-Konten und 25 % der neu eröffneten Konten werden von Betrügern betrieben.[10]

Anwendungsfälle

Im Folgenden haben wir kurz zusammengestellt, welche wichtigen Anwendungsfälle Fertigungsunternehmen mit Fortinet lösen können.



45 % der Unternehmen mit SCADA/ICS-Lösungen verwenden keine rollenbasierte Zugangskontrolle.[14]

Unternehmensinfrastruktur

Fertigungsunternehmen haben ähnliche Anforderungen an die Unternehmens-IT wie andere Branchen: Auch ihr IT-Netzwerk enthält wichtige Daten zu Finanzen, geistigem Eigentum, Personalien, Produktsupport, Außendienst und vielem mehr. Und wie in anderen Branchen sind Hersteller zunehmend auf cloudbasierte Anwendungen und Infrastrukturen angewiesen,[11] während die Anzahl der IoT-Geräte (Internet der Dinge) am Netzwerk-Rand unablässig steigt.[12]

Unabhängig von der Art der sensiblen Daten ist eine umfassende, durchgängig integrierte und automatisierte Cyber-Sicherheitslösung für die Unternehmensinfrastruktur notwendig. Die Fortinet Security Fabric bietet eine solche Lösung, die auf FortiGate Next-Generation-Firewalls (NGFWs) und KI-gestützten Bedrohungsinformationen der FortiGuard Labs basiert. Dazu gehört auch ein offenes Ökosystem. So lassen sich z. B. in die Security Fabric unterschiedlichste Cybersecurity-Tools von Fortinet und Drittanbietern nahtlos über APIs (Application Programming Interface) integrieren.

Air-Gapped-Systeme in der Fertigung

Der Großteil der OT-Systeme ist heute mit IT-Systemen vernetzt. Nach einer aktuellen Forrester-Studie sind aber weiterhin 40 % der OT-Systeme durch ein Air Gap geschützt (also nicht mit anderen Netzwerken verbunden).[13] Man könnte annehmen, dass solche Systeme vor Cyberangriffen sicher seien. Tatsächlich verwenden aber auch Air-Gapped-Systeme IP-basierte Steuerungssysteme und erhalten regelmäßige Software-Updates von externen Dritten. Werden diese Updates bereits beim Software-Anbieter infiziert, können Air-Gapped-Systeme ebenfalls kompromittiert werden. Aber selbst wenn diese Systeme keine sensiblen Daten enthalten, können Angriffe trotzdem kostspielige Betriebsstörungen und Sicherheitsprobleme verursachen.

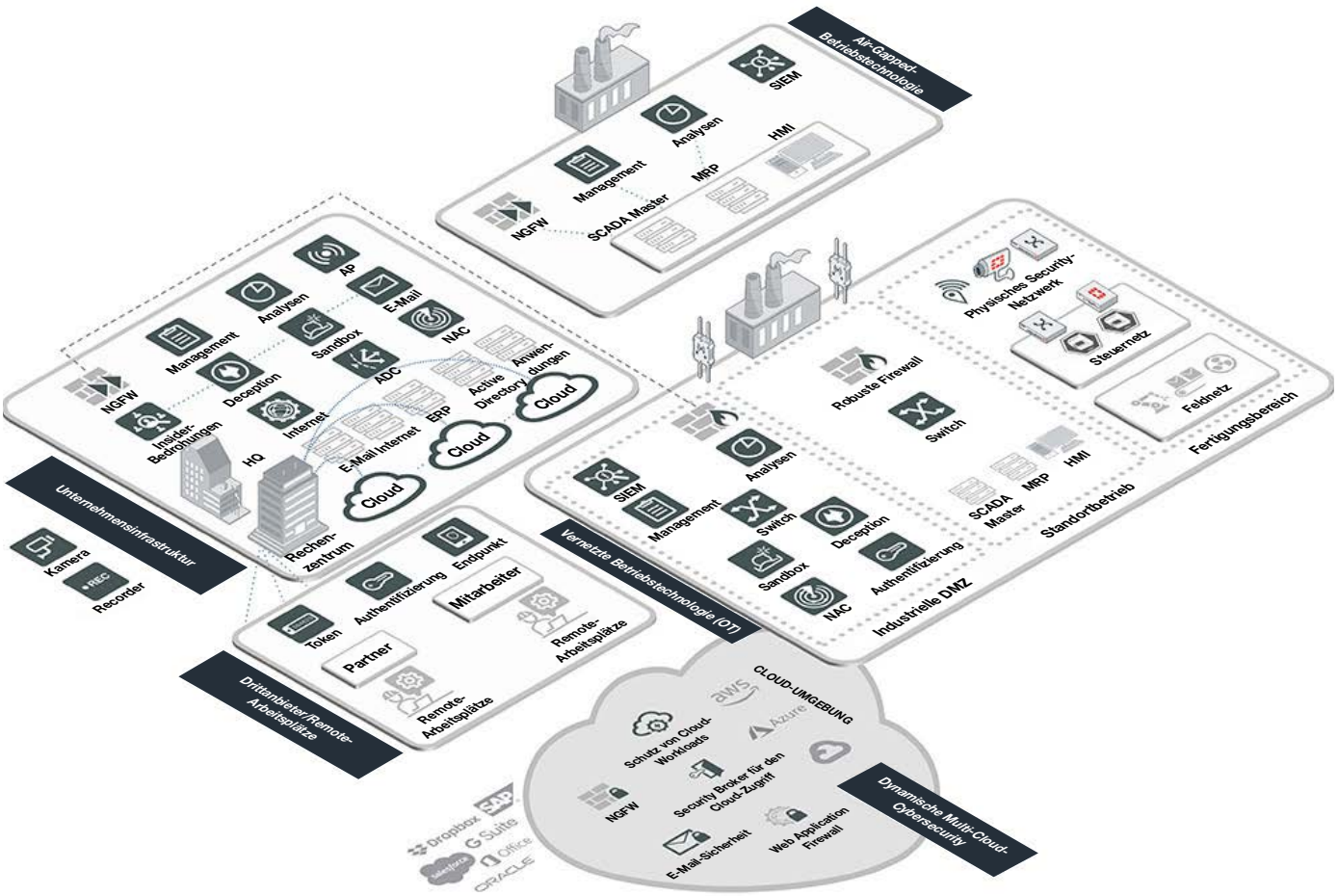
Aus diesen Gründen brauchen auch Air-Gapped-Systeme einen NGFW-Schutz, der mit einem umfassenden Cybersecurity-Tracking und -Reporting einhergehen muss. Das Fortinet-Portfolio enthält dafür geeignete Lösungen: FortiGate NGFWs bieten eine robuste Security und marktführende Leistung bei der Überprüfung von verschlüsseltem und unverschlüsseltem Datenverkehr. Der FortiManager ermöglicht ein zentrales Management, ergänzt durch mehrere Reporting-Tools. Der FortiAnalyzer unterstützt die Cybersecurity und das Log-Management, damit Unternehmen von maximaler Transparenz und einer besseren Erkennung von Sicherheitsverletzungen profitieren. Und mit FortiSIEM – einem Tool für Cybersecurity-Informationen und das Event Management – lassen sich Sicherheitsinformationen und Ereignisdaten aggregieren, um eine koordinierte, automatisierte Reaktion auf Angriffe zu erhalten.

Vernetzte Fertigungssysteme

Wie bereits erwähnt, führen die digitale Transformation und die notwendige geschäftliche Agilität zu einer wachsenden Co-Abhängigkeit von IT und OT. Von industriellen IoT-Sensoren, die Fertigungsabläufe überwachen, bis hin zu Systemen, die öffentlich verfügbare Daten aus dem Internet in die Entscheidungsfindung einbinden, wird Betriebstechnologie zunehmend vernetzt und verliert ihren isolierten Status. Aus Sicht der Cyber-Sicherheit entsteht durch diese Konvergenz eine stark erweiterte Angriffsfläche, auf die OT-Systeme wegen seltener Upgrades denkbar schlecht vorbereitet sind. Diese schwache OT-Cybersecurity setzt Hersteller kurzfristig einem Risiko aus.

Können diese Cyber-Sicherheitsprobleme gelöst werden, lassen sich IT- und Automatisierungsnetzwerke in vielen Fällen zu einer einzigen sicheren und gut verwaltbaren Umgebung konvergieren. Cybersecurity-Teams brauchen dafür allerdings eine Übersicht über alle Systeme, zentrale Kontrolle über WLAN- und LAN-Netzwerke sowie Funktionen, um das Netzwerk je nach Geschäftsanforderungen zu segmentieren.

Die Fortinet Security Fabric schützt die gesamte Angriffsfläche. Diese Sicherheitsstruktur bietet einen umfassenden Überblick darüber, wer sich im Netzwerk befindet und was ein Benutzer (oder Gerät) dort macht. Unternehmen erhalten eine integrierte Kontrolle über jedes System und können so sicherstellen, dass jedes System wirklich „nur tut, was es soll“. Außerdem lässt sich mit der Security Fabric eine intelligente Segmentierung realisieren, um bekannte und unbekannte Bedrohungen automatisch abzuwehren. Die Grundlage der Security Fabric bilden FortiGate NGFWs und KI-gestützte Bedrohungsinformationen der FortiGuard Labs. Ergänzend können zudem zahlreiche Cybersecurity-Tools von Fortinet und seinen Fabric-Partnern nahtlos integriert werden.



Mit den Cybersecurity-Lösungen von Fortinet erhalten Unternehmen eine durchgängige, integrierte Security-Architektur für IT, OT und die physische Sicherheit. Alles wird geschützt – von der Unternehmenszentrale bis zur Produktionsstätte, einschließlich interne Anwender und externe Benutzer von Partnern.

Management von Drittanbietern

Mit dem Trend zum MaaS-Modell (Manufacturing-as-a-Service) in der Fertigung[15] erhalten Drittanbieter in noch nie da gewesenem Umfang Zugriff auf Unternehmensnetzwerke und Betriebstechnologie-Systeme (OT). Fertigungsunternehmen können sich daher nicht mehr „ein für allemal" auf die Vertrauenswürdigkeit eines Benutzers verlassen, sondern müssen prüfen, ob die Security sowohl Schutz vor Insider-Bedrohungen als auch vor unternehmensexternen Dritten bietet. Entscheidend ist, dass man das Cyber-Sicherheitsprofil jedes Partners regelmäßig überprüfen kann. Außerdem benötigen Unternehmen einen robusten Schutz vor Insider-Bedrohungen, der alles abdeckt: versehentliche Sicherheitsverstöße, böswillige Absichten, Gefahren aus dem eigenen Unternehmensnetzwerk sowie Bedrohungen aus den Netzwerken von Partnern.

Die integrierten Lösungen der Fortinet Security Fabric bieten einen mehrstufigen Schutz vor diesen Bedrohungen. Absichtsbasierte Segmentierungsfunktionen in FortiGate NGFWs ermöglichen Herstellern, ihr Netzwerk intelligent zu segmentieren und die Vertrauenswürdigkeit dynamisch zu regeln. Diese Segmentierung stellt zugleich die Grundlage für die Identitäts- und Zugangsverwaltung mit dem FortiAuthenticator sowie für FortiTokens dar: Benutzer erhalten nur Zugriff auf die Netzwerk-Bereiche, die sie unbedingt für ihre Arbeit brauchen. FortiInsight nutzt Benutzer- und Entitätsverhaltensanalysen (UEBA), um Anomalien im erwarteten Verhalten vertrauenswürdiger Benutzer sowie Entitäten zu erkennen, die auf ein kompromittiertes Konto hinweisen. Und FortiDeceptor arbeitet mit einer Deception-Technologie, um interne und externe Angriffe mit Täuschungsmanövern zu enttarnen und proaktiv abzuwehren.

Multi-Cloud-Cybersecurity

Hersteller führen derzeit in kürzester Zeit cloudbasierte Dienste ein[16] und viele arbeiten mittlerweile mit cloudbasierten Systemen für das Manufacturing Resource Planning (MRP) und Enterprise Resource Planning (ERP). Diese Systeme zur Planung von Fertigungs- und Unternehmensressourcen beziehen oft Daten aus IT- und OT-Systemen, um schnelle, effektive Entscheidungen zu unterstützen – ein Prozess, der als „digitales Twinning" bezeichnet wird. Cloudbasierte Lösungen werden zudem routinemäßig für Dienste verwendet, die sich auf die Kundenerfahrung auswirken. Für diese Ressourcen ist die Aufrechterhaltung der Cyber-Sicherheit entscheidend. Folglich muss die integrierte Cybersecurity-Architektur eines Unternehmens vom Rechenzentrum über die Betriebstechnologie bis hin zu mehreren Clouds alles abdecken.

Die Fortinet Security Fabric ermöglicht einen umfassenden Schutz für Multi-Cloud-Umgebungen. Sie gewährleistet ein einheitliches Richtlinien- und Konfigurationsmanagement sowie die Erkennung und Abwehr von Bedrohungen für die gesamte Angriffsfläche. FortiGate VM ist eine Next-Generation-Firewall (NGFW), die als virtuelle Maschine (VM) implementiert wird und ideal für Cloud-Umgebungen geeignet ist. FortiWeb schützt als Web Application Firewall (WAF) speziell die Anwendungsebene mit sicherheitsrelevanten, KI-gestützten Bedrohungsinformationen und ist in verschiedenen Formfaktoren erhältlich.

Beim FortiCASB handelt es sich um einen CASB-Dienst (Cloud Access Cybersecurity Broker). Dieser Dienst bietet Einblicke in Ressourcen, Benutzer, Verhaltensweisen und Daten, die in der Cloud gespeichert sind. Für die Auswertung gibt es umfassende Reporting-Tools. Mit FortiCASB lassen sich zudem Richtlinienkontrollen auf IaaS-Ressourcen (Infrastructure-as-a-Service) und SaaS-Anwendungen (Software-as-a-Service) erweitern. Eigens für den Schutz von Cloud-Workloads hat Fortinet FortiCWP entwickelt (Cloud Workload Protection). Hiermit können Cybersecurity- und DevOps-Teams das Sicherheitsprofil ihrer Cloud-Konfiguration bewerten und potenzielle Risiken durch Fehlkonfigurationen identifizieren.

Alleinstellungsmerkmale: Warum Fortinet?

Warum Fortinet für die Cyber-Sicherheit in der Fertigung die beste Wahl ist

Mit den Lösungen von Fortinet erhalten Hersteller einen Komplettschutz für OT- und IT-Netzwerke. Fortinet-Security-Lösungen unterscheiden sich dabei in wichtigen Punkten von anderen Angeboten auf dem Markt:

- **Integration**
  Die Fortinet-Technologie bietet Herstellern eine durchgängige, integrierte Cybersecurity-Architektur, die alles abdeckt: IT, OT, Cyber-Sicherheit, physische Security, Produktionsstätten, Unternehmenszentrale, Rechenzentrum und mehrere Clouds. Unternehmen können die Sicherheit einheitlich automatisieren und Sicherheitsabläufe genau abstimmen – vom Schutz bis zur Erkennung und Reaktion.
- **Monitoring und Management**
  Mit Fortinet können Hersteller Netzwerk-, Cybersecurity- und Überwachungsfunktionen über ein einziges System steuern. Eine zentrale Konsole sorgt für umfassende Transparenz und Kontrolle. So lassen sich cyberphysische Angriffe verhindern und isolierte Bereiche mit unterschiedlichen Zuständigkeiten vermeiden.
- **Robuste Hardware**
  Hardware muss in Fertigungsumgebungen einiges aushalten können. Wird z. B. eine Firewall-Appliance beschädigt, kann das den gesamten Werksbetrieb zum Erliegen bringen. Fortinet bietet eine breite Auswahl an robusten Appliances, um allen Umgebungsanforderungen gerecht zu werden und einen kontinuierlichen Geschäftsbetrieb zu gewährleisten.
- **Proaktiver Schutz vor Insider-Bedrohungen**
  Das Risikomanagement von Bedrohungen aus dem eigenen Unternehmen wird erheblich komplexer, wenn immer mehr Drittanbieter und Partner Zugang zum Netzwerk erhalten. Fortinet bietet eine umfassende Lösung zum Schutz vor Insider-Bedrohungen. Dazu gehören eine robuste absichtsbasierte Segmentierung, ein Identitäts- und Zugangs-Management (IAM) sowie Benutzer- und Entitätsverhaltensanalysen (UEBA).

Sicherheitsvorfälle in der Fertigung[17] (in den letzten 12 Monaten)

- Malware: 61 %
- Spyware: 45 %
- DDoS-Angriffe: 28 %
- Insider-Bedrohungen: 26 %
- Phishing: 24 %
- Angriffe über Mobilgeräte: 21 %
- Ransomware: 21 %
- Man-in-the-Middle-Angriffe: 18 %
- Zero-Day-Angriffe: 17 %
- SQL-Injektion: 8 %

Folgen der Sicherheitsvorfälle für die Fertigung[17] (in den letzten 12 Monaten)

- Betriebsausfälle mit Produktionsverlust: 45 %
- Schädigung des Marken-Images: 40 %
- Betriebsausfälle mit Gefährdung der physischen Sicherheit: 35 %
- Betriebsausfälle mit Umsatzeinbußen: 32 %
- Verlust geschäftskritischer Daten: 26 %

- **Bedrohungsinformationen speziell für Betriebstechnologie**
  Die FortiGuard Labs liefern zuverlässige Bedrohungsinformationen speziell für OT-Systeme, damit Hersteller bessere strategische Entscheidungen treffen können. Fortinet arbeitet bereits seit 15 Jahren eng mit Fertigungsunternehmen zusammen.
- **Ökosystem der Security Fabric**
  Neben dem breiten Portfolio an Security-Tools lassen sich spezielle OT-Lösungen nahtlos in die Fortinet Security Fabric über das Fortinet Fabric-Partner-Ökosystem einbinden. Alle Daten sind dann in einer zentralen Ansicht verfügbar, um fundierte Entscheidungen zu unterstützen.

Fazit

In einem sich schnell weiterentwickelnden Markt, der eine Just-in-Time-Produktion erfordert, können es sich Hersteller nicht leisten, durch Cybersecurity-Vorfälle – oder zu stark eingreifende Sicherheitsfunktionen – wertvolle Zeit zu verlieren. Die Fortinet Security Fabric bietet eine einheitliche Plattform, die alles schützt: IT, OT und den physischen Zugang zu Produktionsstätten und -systemen. Fertigungsunternehmen profitieren mit Fortinet von umfassender Transparenz und integrierter Kontrolle über eine einzige „Schaltzentrale“.

„CEOs und das leitende Management … sind sich einig, dass sich Strategien auszahlen, die die Markteinführung beschleunigen, die Produktqualität verbessern und Kundenbedürfnisse stärker berücksichtigen.“[18]

„Trotz saisonaler Schwankungen und unterschiedlichster Angriffsziele ist eines klar: IT-basierte Angriffe auf OT-Systeme nehmen zu.“[19]

[1] Marco Annunziata: „Manufacturing-As-A-Service Platforms: The New Efficiency Revolution“. Forbes, 13. Mai 2019.

[2] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 8. Mai 2019.

[3] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit“. Fortinet, 10. September 2019.

[4] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 8. Mai 2019.

[5] „Cyber Physical Systems Security“. Department of Homeland Security, abgerufen am 7. November 2019.

[6] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 8. Mai 2019.

[7] „Q3 Fraud and Abuse Report“. Arkose Labs, 18. September 2019.

[8] „Ninth Annual Cost of Cybercrime Study“. Accenture und Pomenon Institute, 6. März 2019.

[9] Elizabeth Montalbano: „Six Cyber-Physical Attacks the World Could Live Without“. The Security Ledger, 18. Januar 2017.

[10] „Q3 Fraud and Abuse Report“. Arkose Labs, 18. September 2019.

[11] Louis Columbus: „10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018“. Manufacturing Business Technology, 23. Februar 2018.

[12] „Applications of IoT in Manufacturing Plants“. The Manufacturer, 12. April 2018.

[13] „Independent Study Pinpoints Significant SCADA/ICS Security Risks“. Fortinet, 16. April 2019.

[14] Ebd.

[15] Marco Annunziata: „Manufacturing-As-A-Service Platforms: The New Efficiency Revolution“. Forbes, 13. Mai 2019.

[16] Louis Columbus: „10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018“. Manufacturing Business Technology, 23. Februar 2018.

[17] Basierend mehreren Erhebungen von Fortinet mit verschiedenen Personas. Berichte zu den Studien erscheinen in Kürze.

[18] Louis Columbus: „10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018“. Manufacturing Business Technology, 23. Februar 2018.

[19] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 8. Mai 2019.

FORTINET

www.fortinet.com/de

20. Juni 2022, 10:54
517972-A-1-DE