FORTINET

WHITEPAPER

# Schutz von OT-Systemen vor sich schnell weiterentwickelnden Bedrohungen

## Was CISOs mit Betriebstechnologie über die komplexe Bedrohungslage wissen müssen

## Zusammenfassung

**In vielen Unternehmen mit kritischer Betriebstechnologie (OT) werden beim Management dieser Systeme – und ihrer Sicherheit – seit Jahrzehnten die gleichen Praktiken befolgt. Das Problem: Ein Großteil der heute aktiven Industrieanlagen wurde zu Zeiten entwickelt, als OT- und IT-Systeme noch durch den so genannten „Air Gap" getrennt waren. Diesen schützenden „Luftspalt" gibt es nicht mehr. OT-Systeme sind mittlerweile mit IT-Netzwerken und dem Internet verbunden und dadurch hochkomplexen Bedrohungen ausgesetzt, die veraltete OT-Security-Lösungen oft weder erkennen noch abwehren können. Angriffe auf OT-Systeme werden daher für viele Chief Information Security Officer (CISOs) zur Achillesferse, da dabei größerer Schaden angerichtet werden kann als bei einer „normalen" Datenpanne oder durch Ransomware. Zusätzlich zu finanziellen Verlusten und Image-Schäden können kompromittierte OT-Systeme auch die Produktivität beeinträchtigen, Betriebskapital wie Fertigungsanlagen schädigen und Sicherheitsrisiken für Mitarbeiter und andere Personen bedeuten.**

**Für 94 % der Befragten aus Unternehmen mit Betriebstechnologie ist das OT-Sicherheitsprofil ein wichtiger oder mittlerer Faktor bei der Bewertung des Geschäftsrisikos, die der CISO der Geschäftsleitung und dem Vorstand vorlegen muss.[4]**

## Wachsende Bedrohung von OT-Unternehmen durch Angriffe

Durch Modernisierungen und den verstärkten Einsatz von IIoT-Technologien (IIoT = Industrial Internet of Things) wird der „Air Gap" – der schützende „Luftspalt" zwischen Informationstechnologie (IT) und Betriebstechnologie (OT) – sukzessive aufgelöst. Die Folge ist eine ständig wachsende Angriffsfläche. OT-Sensoren werden zunehmend in IT-Netzwerke integriert, um eine Schnittstelle zu maschinellem Lernen (ML) und Big-Data-Technologien zu schaffen. Diese Konnektivität bringt zwar Wettbewerbsvorteile für das Unternehmen, erhöht jedoch zugleich die Gefahr illegaler Netzwerk-Zugriffe. Besonders problematisch sind die wachsenden Schwachstellen, weil unüberwachte Betriebstechnologie nicht auf Sicherheit ausgelegt ist und keine Standardsoftware wie Security-Clients ausführen kann. Da die Anlagen immer laufen müssen, sind die Zeitfenster für Security-Updates oft eng bemessen. Die Folge ist, dass nur die kritischsten Patches installiert werden.

Angriffe auf OT-Systeme setzen ein Unternehmen ernsthaften Risiken aus: Womöglich will ein Eindringling gar keine Daten stehlen, sondern Anlagen manipulieren oder lahmlegen. Doch unabhängig davon, ob ein Angreifer eine Produktionslinie herunterfahren, eine kritische Prozessüberwachung deaktivieren oder ein Ventil öffnen will, das geschlossen bleiben muss – ein solcher Angriff kann für das Unternehmen und seine Kunden verheerende Folgen haben. Angriffe auf Betriebstechnologie können aber auch darauf abzielen, über das gemeinsame IT-OT-Netzwerk in die IT-Systeme des Unternehmens einzudringen. Man spricht dann von einer seitlichen oder lateralen Bewegung. Die Logik dahinter ist simpel: Ist die OT-Abwehr schwach, kann ein Angreifer dort leichter eindringen und sich dann bis zu personenbezogenen Kundendaten oder vertraulichen Finanzinformationen „vorarbeiten".

Fast drei Viertel der OT-Unternehmen haben in den letzten 12 Monaten mindestens einen illegalen Netzwerk-Zugriff erlebt, die Hälfte verzeichnete sogar drei oder mehr Angriffe.[1] Zudem sind fast allen Unternehmen (97 %) mit SCADA- und ICS-Technologien die Sicherheitsprobleme bewusst, die die Konvergenz von IT und OT mit sich bringt.[2] Einige Angriffe auf Betriebstechnologie verwenden „umfunktionierte" Malware: Wird der Angriff von der IT-Security erfolgreich abgewehrt, wird die gleiche Malware erneut gegen schlechter geschützte OT-Systeme eingesetzt.[3] Allerdings steigt der Anteil der Angriffe auf OT-Systeme, die eigens für die Sicherheitsvorkehrungen von Betriebstechnologie entwickelt wurden.

## Weiterentwicklung einer ständig wachsenden Bedrohungslandschaft

Spezielle OT-Angriffe zielen auf die größten Schwachstellen von OT-Netzwerken ab. Oft sind das die kleinsten, simpelsten Infrastruktur-komponenten wie Bridges oder serielle Wandler.[5] Industroyer, ein Malware-Angriff, der 2016 das ukrainische Stromnetz zum Erliegen brachte, griff z. B. Schutzrelais an.

Der mehrgleisige Angriff nahm seinen Anfang bei einer bekannten Sicherheitslücke in von Siemens hergestellten Relais für digitale Umspannwerke.[6] Über diese Schwachstelle gelangte die Malware in ein OT-Netzwerk von Geräten für die Stromversorgung in Kiew. Erst wurden zwei Backdoor-Netzwerk-Zugriffspunkte erstellt, dann folgte die gleichzeitige Implementierung auf allen erreichbaren Leistungsschaltern und Schutzrelais sowie auf den Windows-Workstations, auf denen die ABB MicroSCADA-Software zur Steuerung dieser Geräte lief.

Der Angriff wurde mit einem Timer gesteuert. Als der festgelegte Zeitpunkt erreicht war, erfolgte ein DDoS-Angriff (Distributed Denial-of-Service) auf jedes Schutzrelais im Netzwerk, das eines von vier Kommunikationsprotokollen verwendete.[7] Gleichzeitig wurden alle MicroSCADA-Dateien von den Festplatten der Workstations gelöscht. Die unmittelbare Folge war, dass die Relais im gesamten Netzwerk nicht mehr reagierten und in ganz Kiew der Strom ausfiel. Doch damit nicht genug: Noch Jahre später gab es weltweit Angriffe auf OT-Geräte mit Industroyer.[8]

Der Trend zu speziellen OT-Angriffen setzt sich seitdem fort. Heute zielen 85 % aller OT-Bedrohungen auf eines von drei OT-Steuerprotokollen ab:[9] OPC Classic ist das am häufigsten verwendete OT-Protokoll aus den 90er und 2000er Jahren. Systeme, die mit diesem Protokoll arbeiten, sind für Angreifer attraktiv, weil sie so weit verbreitet sind. An zweiter Stelle steht BACnet von 1987, das viele Heizungs-, Lüftungs- und Klimaanlagen (z. B. von Johnson Controls und Carrier) verwenden. Im Jahr 2018 betrafen die drei größten Bedrohungen – nach der Anzahl der Geräte – alle das BACnet-Protokoll.[10] Das dritte ist das OT-Kommunikationsprotokoll Modbus, das 1979 entwickelt wurde – in der Annahme, dass Betriebstechnologie immer durch einen „Air Gap" geschützt bliebe. Bei Modbus kommt erschwerend hinzu, dass es zahlreiche Iterationen von unterschiedlichsten Anbietern gibt und das Verfolgen selbst bekannter Modbus-Schwachstellen extrem zeitaufwändig ist.[11]

Eine weitere Herausforderung für OT-Security-Manager besteht darin, dass Angriffe häufig zu Spitzenzeiten stattfinden, um den größten Schaden anzurichten oder – im Fall einer Erpressung – maximalen Druck auf das Unternehmens auszuüben, das für die Sicherheitslücke verantwortlich ist. In Nordamerika nehmen z. B. Angriffe auf Klimaanlagen und Stromnetze während der Sommermonate zu.[12]

**Bedrohungen werden immer ausgefeilter – und schwerer zu erkennen**

Kein Anbieter von SCADA- oder anderen ICS-Systemen ist gegen diese Risiken gefeit. Laut einer Fortinet-Studie von 2019 zu OT-Bedrohungen wurden Geräte von Advantech, Schneider Electric, Moxa und Siemens zwar am häufigsten angegriffen, aber bei allen der 70 untersuchten OT-Anbieter waren ständige Angriffe die Regel.[14] Weiter zeigte die Studie, dass die Anzahl und Häufigkeit der Angriffe für fast jeden SCADA- und ICS-Anbieter zunimmt.

Diese Attacken werden immer gezielter: Mit einem mehrstufigen Angriffsplan soll ein konkretes Ergebnis bei einem bestimmten Unternehmen erreicht werden. Industroyer ist dafür ein typisches Beispiel. In Kiew lief der Angriff über mehrere Monate und wurde dann gezielt an einem bestimmten Tag ausgelöst. (Annahmen zufolge steckte Russland dahinter, um Kiew während der Invasion in der Ukraine zu schwächen.) Zudem umfasste der Angriff mehrere Schritte: das Eindringen in das OT-Netzwerk über die Siemens-Relais, die Schaffung von zwei separaten Backdoor-Zugriffspunkten, die netzwerkweite Implementierung auf OT-Geräten und Workstations und die anschließende Aktivierung.

**„Komplexe Malware wie Industroyer hat in der Regel eine lange Lebensdauer – selbst nachdem eine Bedrohungserkennung und Signaturen implementiert wurden."[13]**

**„Viele Angreifer schleusen Malware nicht mehr ein, um auf möglichst vielen Systemen Chaos anzurichten, sondern um sich genau über industrielle Steuerungstechnik zu informieren mit dem Ziel, bestimmte Branchen, Länder und Unternehmen anzugreifen."[17] – Mark Carrigan, Chief Operating Officer von PAS Global**

Die Erkennung und Abwehr von OT-Angriffen wird zunehmend schwerer. Häufig umfasst Malware auch Funktionen, die einen Antivirus- oder Bedrohungsschutz aushebeln: Malware kann z. B. erkennen, ob sie in einer Sandbox-Umgebung ausgeführt wird, Sicherheits-Tools auf infizierten Computern deaktivieren oder Junk-Daten verbreiten, um ihre Entfernung zu erschweren.[15] Immer mehr der gegen Betriebstechnologie gerichteten Malware tarnt sich auch mit Verschlüsselungen. So haben Security Researcher hochentwickelte Ausweichtaktiken wie z. B. bei der Ransomware Ryuk entdeckt, die ihren eigenen Kodierungsschlüssel zerstört und Schattenkopien von infizierten Systemen löscht.[16]

**Angriffe auf Triconex-Systeme blieben monatelang unbemerkt**

TRITON-Angriffe – auch als TRISIS bekannt – zielen auf von Schneider Electric entwickelte SIS-Steuerungen (Triconex Safety Instrumented System) ab. Der erste bekannte TRITON-Exploit galt einer petrochemischen Anlage in Saudi-Arabien. Die Malware gelangte auf unbekanntem Weg (wahrscheinlich über Phishing) in das IT-Netzwerk des Unternehmens.[18] Vom internen IT-Bereich bewegten sich die Angreifer seitlich im Netzwerk bis zum OT-Bereich. Obwohl bei der Anlage eine DMZ-Architektur (Demilitarized Zone) implementiert war, die IT- und OT-Netzwerke durch eine Firewall trennte, initiierten die Angreifer vom IT-Netzwerk aus RDP-Sitzungen (Remote Desktop Protocol) zu den Engineering-Workstations der Anlage.[19]

Bei dem ersten bekannten Vorfall, bei dem eine technische Abteilung angegriffen wurde,[20] hatte sich TRITON/TRISIS anscheinend auf die Netzwerk-Reconnaissance konzentriert. Die Angreifer stahlen keine Daten, machten keine Screenshots und protokollierten keine Tastenanschläge.[21] Stattdessen sammelten sie mit der Malware Anmeldedaten von Benutzern, um im IT- und OT-Netzwerk Backdoors zu erstellen. Über diese Hintertüren erlangten sie dann Zugriff auf die SIS-Engineering-Workstations. Die Malware benannte außerdem ihre eigenen Dateien um, sodass sie wie Microsoft-Updates aussah, und verwendete sowohl Webshells als auch SSH-Tunnel (Secure Shell).[22]

Die Angreifer erhielten Zugriff auf das Distributed Control System (DCS) der Anlage, scheinen sich jedoch ausschließlich auf die SIS-Controller konzentriert zu haben.[23] Letztlich scheiterte der ausgefeilte Plan dennoch: Die sechs infizierten Triconex SIS-Systeme wurden vor dem geplanten Angriffszeitpunkt heruntergefahren, was vermutlich durch eine versehentliche Aktivierung der Malware ausgelöst wurde.[24] Die Systeme gingen darauf in einen „Fail-Safe"-Zustand und die Katastrophe wurde abgewendet.[25]

Der Angriff zeigt jedoch, inwieweit ein ambitionierter Hacker mit einem facettenreichen Angriff voller hochentwickelten Methoden (z. B. Ändern von Dateinamen, Entwickeln und Bereitstellen von SSH-Tunneln, Erstellen mehrerer Backdoors für den Netzwerk-Zugriff) Standard-Sicherheitsmaßnahmen umgehen kann. Tatsächlich war die Malware derart schwer zu erkennen, dass der erste Angriffsversuch – ein Herunterfahren eines einzelnen Triconex-SIS-Systems im selben Werk zwei Monate zuvor – unentdeckt blieb. Schneider Electric hatte damals anhand der Protokolldateien seines Systems die erfassten Daten diagnostiziert und das Problem als mechanischen Fehler eingestuft.[26]

**Unbekannte Angriffsformen und Zero-Day-Exploits werden oft ignoriert**

Bekannte Malware kann schwierig zu erkennen sein, wenn sie so komplex wie der TRITON/TRISIS-Angriff ist. Tatsächlich hat TRITON/TRISIS im April 2019 ein zweites Opfer im Nahen Osten kompromittiert.[28] Berichten zufolge griff die Gruppe hinter TRITON/TRISIS Anfang 2019 auch mehrere nordamerikanische Öl- und Gasziele an.[29]

Erfolgreiche bekannte Malware ist jedoch nicht das einzige Risiko für OT-Systeme. Neue innovative Angriffsformen kommen laufend dazu. Ein Beispiel ist LockerGoga, ein Ransomware-Programm, das im März 2019 weltweit die Produktion in Norsk Hydro-Aluminiumwerken stoppte. Die wichtigste Neuerung bei diesem Angriff war, dass die Malware weder über den Netzwerk-Traffic noch über das Domain Name System (DNS) oder CC-Server (Command and Control) verbreitet wurde[30] – sondern mithilfe der netzwerkeigenen Active-Directory-Dienste.[31] Am Tag nach der erstmaligen Entdeckung von LockerGoga bei Norsk Hydro erkannten nur 17 der 67 marktführenden Virenscanner diese Bedrohung.[32]

## OT-Sicherheitsverletzungen verursachen hohe, dauerhafte Verluste

Die geschäftlichen Auswirkungen von OT-Verstößen können schwerwiegend sein. Einige – wie LockerGoga – sind so konzipiert, dass sie OT-Systeme manipulieren und dann das Unternehmen damit erpressen. Viele zielen jedoch auf das Abschalten oder Beschädigen von Industrieanlagen ab.[34] Ein plötzlicher Produktionsstillstand beeinträchtigt zweifellos die Fähigkeit des Unternehmens, seine Fertigungsziele zu erreichen – möglicherweise sogar über einen längeren Zeitraum.

Jede Ausfallzeit bei einem OT-Systemen kann sofortige Umsatzverluste bedeuten. Je nach Unternehmen kann sich das in nur wenigen Minuten auf sechsstellige oder sogar Millionenbeträge summieren. Beispielsweise kostete ein Produktionsstillstand wegen der NotPetya-Ransomware den Pharmagiganten Merck 2017 fast 1 Milliarde US-Dollar.[35] Und bei der Reederei Maersk verursachte NotPetya einen Volumenrückgang von 20 % mit Einbußen von 300 Millionen US-Dollar.[36] Viele Unternehmen hatten noch ein Jahr später mit den Folgen von NotPetya zu kämpfen.[37]

**„Theoretisch war die Anlagen-Architektur sicher. Aber die DMZ-Infrastruktur war schlecht konfiguriert, sodass Angreifer die DMZ kompromittieren und die Kontrolle über das Netzwerk übernehmen konnten.“[27] – Julian Gutmanis, Principal Threat Analyst bei Dragos Inc.**

**„Jedes Unternehmen mit vernetzten ICS- oder SCADA-Systemen sollte die Bedrohungslage ernst nehmen. Angreifer denken strategisch und schöpfen aus jeder neu entwickelten Bedrohung einen maximalen Wert, indem sie ungeschützte Systeme und Schwachstellen ausnutzen.“[33]**

Auch Umweltschäden können schnell infolge eines Angriffs auf Betriebstechnologie entstehen. Obwohl dies letztendlich nicht geschah, bestand bei dem TRITON/TRISIS-Angriff die Gefahr, dass giftige Schwefelwasserstoffgase freigesetzt werden.[38] Eine solche ökologische Katastrophe würde wahrscheinlich hohe Kosten für die Dekontaminierung und Bußgeldzahlungen zur Folge haben und könnte den Ruf des Unternehmens erheblich schädigen.

Wird Betriebstechnik plötzlich angehalten, besteht zudem für die Gerätebediener und Mitarbeiter die Gefahr einer Verletzung oder sogar Lebensgefahr. Im medizinischen Umfeld erweiterten sich diese Risiken zusätzlich auf Patienten, deren Leben gefährdet sein könnte, wenn eine Maschine wie ein Beatmungsgerät ohne Vorwarnung ausfällt. Die Security-Teams von Krankenhäusern sind zunehmend besorgt über mögliche Angriffe, die den Klinikbetrieb auf diese Weise stören könnten.[39]

Studien zu Cyber-Angriffen auf OT-Unternehmen belegen all diese Folgen: Mehr als einer von vier Befragten (43 %) gab in einer aktuellen Fortinet-Studie an, dass die Produktivität unter den aufgetretenen Betriebsausfälle gelitten hatte. 36 % berichteten von Umweltschäden durch Ausfälle, 23 % von Gefährdungen für Leib und Leben, 30 % von Image-Schäden und 28 % von Verlusten geschäftskritischer Daten.[40]

## Fazit: Abwägen der Risiken

Die Kosten eines OT-Angriffs sind viel zu hoch, um sie zu ignorieren. CISOs in Branchen, die auf betriebliche und industrielle Produktionssysteme angewiesen sind – z. B. in Bereichen wie Fertigung, Versorgung und Transport – stehen zunehmend unter dem Druck, einen angemessenen Schutz der betriebstechnischen Seite ihres Netzwerks sicherstellen zu müssen. Herkömmliche Ansätze für die OT-Security können jedoch nicht mit dem Entwicklungstempo hochkomplexer Bedrohungen Schritt halten.

**Die Ransomware NotPetya kostete Merck fast 1 Milliarde US-Dollar und Maersk 300 Millionen US-Dollar.**[41,42]

Angesichts der potenziell gravierenden Folgen einer Sicherheitsverletzung sollten sich CISOs mehrere Fragen stellen:

- Kann ich darauf vertrauen, dass unsere Security-Anbieter Angriffe auf alle unsere geschäftskritischen OT-Systeme erkennen können?
- Kann unser Unternehmen unbekannte Bedrohungen und Zero-Day-Threats identifizieren?
- Verfügen wir über die richtigen Prozesse, um unerkannte Risiken zu minimieren?
- Bieten unsere Systeme Incident-Response-Technologien, die komplexe, getarnte oder verschleierte Sicherheitsbedrohungen verhindern können?
- Welche möglichen Auswirkungen hat eine Sicherheitsverletzung? Welche Risiken sind am wichtigsten, wenn ich einen Business Case zur Verbesserung der OT-Security erstellen muss?

Ein CISO, der diese Fragen zuversichtlich beantworten kann, ist eher in der Lage, kritische OT-Systeme zu schützen, die für Betriebsabläufe im Unternehmen von fundamentaler Bedeutung sind.

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

[2] „Unabhängige Studie zeigt signifikante Security-Risiken für SCADA/ICS“. Fortinet, 28. Juni 2019.

[3] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

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

[5] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[6] Charlie Osborne: „Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout“. ZDNet, 30. April 2018.

[7] Ebd.

[8] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[9] Ebd.

[10] Ebd.

[11] Ebd.

[12] Ebd.

[13] Ebd.

[14] Ebd.

[15] „Threat Landscape Report Q2 2019“. Fortinet, 2. Quartal 2019.

[16] Ebd.

[17] Robert Lemos: „TRITON Attacks Underscore Need for Better Defenses“. Dark Reading, 15. April 2019.

[18] Thomas Roccia: „Triton Malware Spearheads Latest Generation of Attacks on Industrial Systems“. McAfee, 8. November 2018.

[19] Kelly Jackson Higgins: „Triton/Trisis Attack Was More Widespread Than Publicly Known“. Dark Reading, 16. Januar 2019.

[20] Ebd.

[21] Charlie Osborne: „Triton hackers return with new, covert industrial attack“. ZDNet, 10. April 2019.

[22] Ebd.

[23] Ebd.

[24] Kelly Jackson Higgins: „Triton/Trisis Attack Was More Widespread Than Publicly Known“. Dark Reading, 16. Januar 2019.

[25] Charlie Osborne: „Triton hackers return with new, covert industrial attack“. ZDNet, 10. April 2019.

[26] Kelly Jackson Higgins: „Triton/Trisis Attack Was More Widespread Than Publicly Known“. Dark Reading, 16. Januar 2019.

[27] Ebd.

[28] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[29] „Threat Landscape Report Q2 2019“. Fortinet, 2. Quartal 2019.

[30] Dan Goodin: „'Severe' ransomware attack cripples big aluminum producer“. Ars Technica, 19. März 2019.

[31] Mathew J. Schwartz: „Hydro Hit by LockerGoga Ransomware via Active Directory“. BankInfoSecurity, 20. März 2019.

[32] Dan Goodin: „'Severe' ransomware attack cripples big aluminum producer“. Ars Technica, 19. März 2019.

[33] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[34] Robert Lemos: „TRITON Attacks Underscore Need for Better Defenses“. Dark Reading, 15. April 2019.

[35] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[36] Iain Thomson: „NotPetya ransomware attack cost us $300m“. The Register, 16. August 2017.

[37] Kim S. Nash, et al.: „One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs“. The Wall Street Journal, 27. Juni 2018.

[38] Kelly Jackson Higgins: „Triton/Trisis Attack Was More Widespread Than Publicly Known“. Dark Reading, 16. Januar 2019.

[39] Mark Klimek: „Hospitals face rising risk of sophisticated cyberattacks“. Healthcare Finance, 17. September 2019.

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

[41] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems“. Fortinet, 16. Mai 2019.

[42] Iain Thomson: „NotPetya ransomware attack cost us $300m“. The Register, 16. August 2017.

FORTINET

www.fortinet.com/de



31. August 2020, 8:36 Uhr

370120-0-1-DE