FORTINET

BERICHT

Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit

Inhaltsverzeichnis

Zusammenfassung

Die operative Technologie (OT) ist für die öffentliche Sicherheit und den wirtschaftliche Erfolg von entscheidender Bedeutung, denn sie steuert die Geräte, mit der Produktionsanlagen, Stromnetze, Wasserversorger, Reedereien und vieles mehr betrieben werden.

Der Aufstieg der OT begann in den frühen Jahrzehnten des 20. Jahrhunderts, als elektrisch betriebene Maschinen und Steuerungen dampf- und muskelbetriebene Geräte ersetzten. OT geht somit dem Aufstieg der Informationstechnologie (IT) um viele Jahrzehnte voraus. Daher waren traditionell OT- und IT-Netze durch ein „Air Gap" voneinander getrennt. In jüngster Zeit werden jedoch IT-basierte Technologien wie Sensoren, maschinelles Lernen (ML) und Big Data in OT-Netzwerke integriert, um neue Effizienz- und Wettbewerbsvorteile zu schaffen. Dies vergrößert die digitale Angriffsfläche und damit die Gefahr unerlaubter Zugriffe.

Um den Stand der Cyber-Sicherheit in OT-Umgebungen zu untersuchen, befragte Fortinet Verantwortliche für Anlagenbetrieb und Produktion bei großen Unternehmen aus den Bereichen Fertigung, Energie und Versorgung, Gesundheitswesen und Transport. Die Umfrage ergab u. a. folgende Erkenntnisse:

1. **Die Auswirkungen von Cyber-Angriffen auf OT-Umgebungen sind breit gefächert und tiefgehend.** Etwa 74 % der OT-Unternehmen haben in den letzten 12 Monaten einen Malware-Zugriff erlebt, der Schäden für Produktivität, Ertrag, Markenvertrauen, geistiges Eigentum und physische Sicherheit nach sich zog.

2. **Ein Mangel an Cyber-Sicherheit erhöht das Risiko.** 78 % haben nur zum Teil eine zentralisierte Sichtbarkeit der Cyber-Sicherheit ihrer OT-Umgebungen. 65 % haben keine rollenbasierte Zugriffskontrolle, und mehr als die Hälfte verwendet keine Multi-Faktor-Authentifizierung oder interne Netzwerksegmentierung.

3. **Die Verbesserung des OT-Sicherheitsprofils wird durch die Notwendigkeit erschwert, mit dem schnellen Wandel Schritt zu halten, sowie durch den Mangel an Fachpersonal.** Fast zwei Drittel (64 %) der OT-Verantwortlichen sehen im Schritthalten mit dem Wandel ihre größte Herausforderung, und fast die Hälfte (45 %) sieht sich durch einen Mangel an qualifizierten Arbeitskräften eingeschränkt.

4. **Der Fokus auf Cyber-Sicherheit nimmt in OT-Unternehmen zu.** 70 % planen die Cyber-Sicherheit für OT im nächsten Jahr unter Leitung des CISO zu implementieren (nur 9 % der CISOs überwachen derzeit die OT Security) und 62 % der Cyber-Sicherheitsbudgets sollen erhöht werden.

Dieser Bericht fasst die Umfrageergebnisse zu folgenden Fragen zusammen:

- Herausforderungen, die Verantwortliche für den Anlagenbetrieb beim Schutz ihrer OT-Umgebungen sehen
- Die Art der Eingriffe, mit denen sie es zu tun haben und deren Auswirkungen
- Wie mit Cyber-Sicherheit umgegangen wird
- Welche Sicherheitslücken vorhanden sind
- Wie der Erfolg gemessen wird

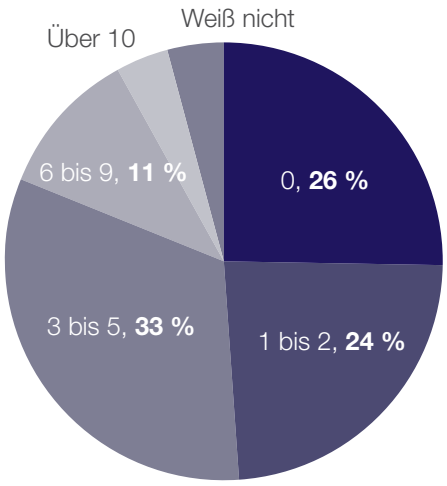
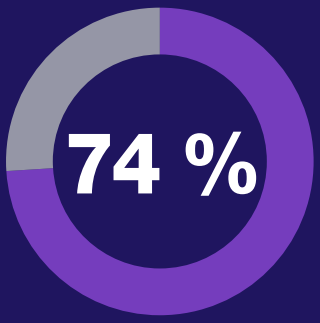
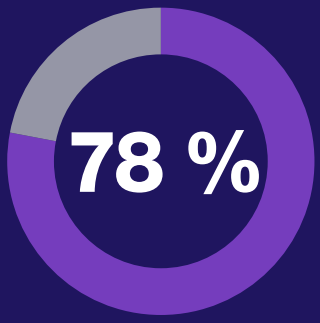


Abbildung 1. Anzahl der unbefugten Zugriffe in den letzten 12 Monaten

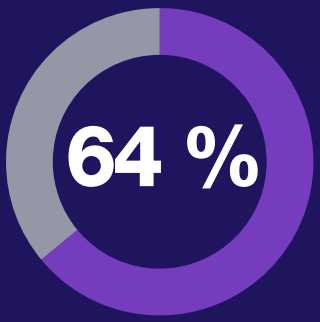
Infografik: Wichtige Erkenntnisse zur OT-Cyber-Sicherheit



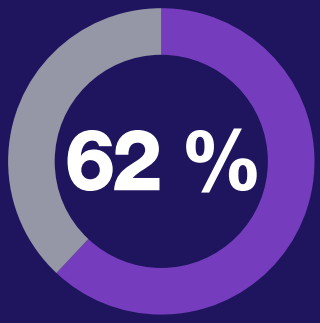
der befragten OT-Unternehmen haben in den letzten 12 Monaten eine Datenschutzverletzung erlebt, die zu Datenverlust, Betriebsstörungen oder Ausfällen und/oder einer Markenschädigung führte.



haben eingeschränkte zentralisierte Sichtbarkeit der Cyber-Sicherheit.



haben Schwierigkeiten, mit dem Wandel Schritt zu halten.



erhöhen ihre Cyber-Sicherheitsbudgets.

Schädigungen durch Datenschutzverletzungen

- Produktivität (43 %)
- Ertrag (36 %)
- Markenreputation (30 %)
- Geschäftskritische Daten (28 %)
- Sicherheitsrisiko (23 %)

70 % planen, **Cyber-Sicherheit unter Leitung des CISO** im nächsten Jahr zu implementieren.

Allerdings sind derzeit nur 9 % der CISOs für die OT-Cyber-Sicherheit verantwortlich.

Im Vergleich zu weniger geschützten OT-Unternehmen (mindestens 6 unbefugte Zugriffe in 12 Monaten) gilt für Unternehmen mit hervorragender OT-Security (null unbefugte Zugriffe in 12 Monaten):

100 % verwenden Multi-Faktor-Authentifizierung

94 % verwenden rollenbasierte Zugriffskontrolle

68 % verwalten und überwachen Sicherheitsereignisse und führen Ereignisanalysen durch

51 % verwenden Netzwerksegmentierung

46 % planen Sicherheits-Überprüfungen

Methodik dieser Studie

Der Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit basiert auf einer Umfrage vom Januar 2019 unter Personen, die:

- in Unternehmen mit mehr als 2500 Mitarbeitern in den Bereichen Fertigung, Energie und Versorgung, Gesundheitswesen und Transport arbeiten.
- OT als ihre Hauptverantwortungsbereich haben.
- für die Berichterstellung zu den Betriebsabläufen verantwortlich sind.
- an Kaufentscheidungen für Cyber-Sicherheit beteiligt sind.

Erkenntnisse zur Cyber-Sicherheit für die operative Technologie (OT)

Erkenntnis: Die Auswirkungen von OT-Cyber-Angriffen sind breit gefächert und schwerwiegend

Fast drei Viertel (74 %) der OT-Unternehmen erlebten im vergangenen Jahr mindestens einen Malware-Zugriff, und die Hälfte (50 %) verzeichnete 3 bis 10 oder mehr unbefugte Zugriffe.

Wie Abbildung 2 zeigt, ist Malware die vorrangige Form unbefugter Zugriffe, gefolgt von Phishing (45 %), Spyware (38 %) und Datenschutzverletzungen bei der mobilen Sicherheit (28 %).

Die Auswirkungen von Datenschutzverletzungen bei OT-Unternehmen sind schwerwiegend, wie in Abbildung 3 dargestellt.

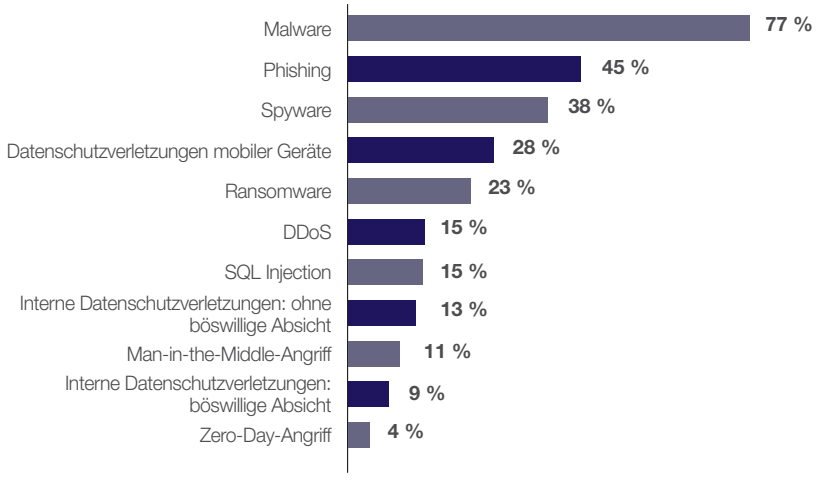


Abbildung 2. Art der erlebten unbefugten OT-Zugriffe

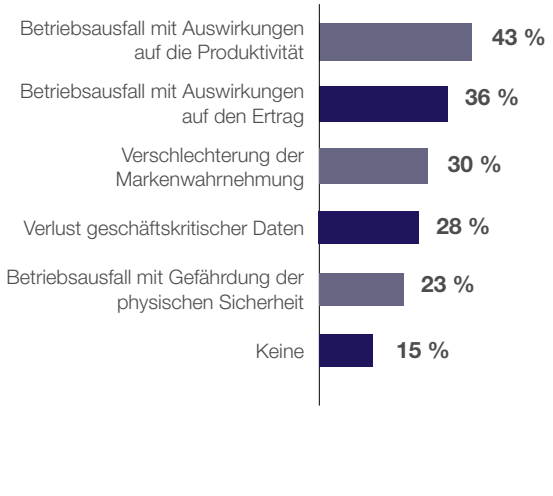


Abbildung 3. Auswirkungen von Datenschutzverletzungen in OT-Unternehmen

Erkenntnis: Mangelnde Sichtbarkeit der Cyber-Sicherheit erhöht das Risiko

78 % der Unternehmen haben nur eine zum Teil zentralisierte Sichtbarkeit der Cyber-Sicherheit ihrer OT-Abläufe, wie in Abbildung 4 dargestellt.

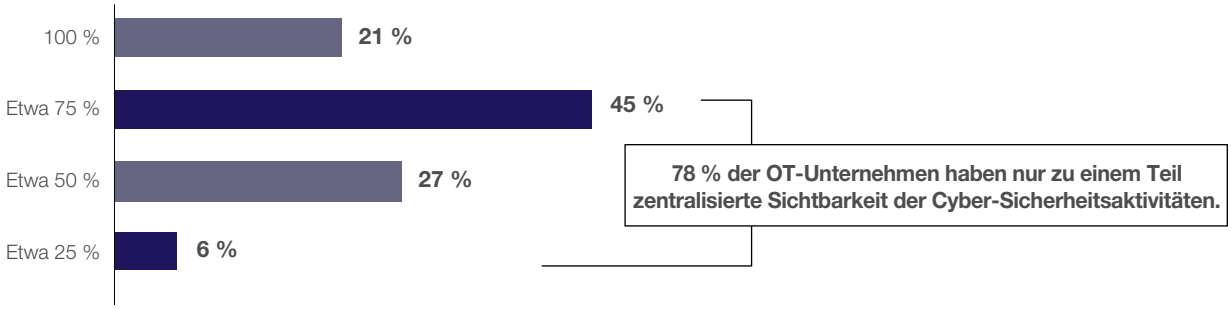


Abbildung 4. Anteil der zentral sichtbaren OT-Cyber-Sicherheitsaktivitäten in Prozent

Erkenntnis: Mangel an qualifizierten Mitarbeitern ist ein zentrales Problem bei der Verbesserung der Cyber-Sicherheit

Fast zwei Drittel der Verantwortlichen für den Anlagenbetrieb (64 %) sehen ihre größte Herausforderung darin, mit dem Wandel Schritt zu halten, gefolgt von einer Vielzahl weiterer Herausforderungen wie:

- Gewerkschaftsbeziehungen (45 %)
- Fachkräftemangel (45 %)
- Änderungen der Compliance-Vorschriften (44 %)
- Verfügbarkeit und Zugang zu Schulungen (42 %)
- Budgetbeschränkungen (42 %)

Darüber hinaus ist der Mangel an Fachkräften ein Faktor bei den vier größten Herausforderungen, die Verantwortliche von Anlagenbetreibern bei der Erweiterung ihrer Cyber-Sicherheitslösungen sehen:

- Schaffung größerer Komplexität (53 %)
- Forderung nach anspruchsvollen Security-Standards (45 %)
- Forderung nach mehr Mitarbeitern im operativen Bereich (45 %)
- Beeinträchtigung der betrieblichen Flexibilität (44 %)

Weitere Daten zeigen jedoch, dass die OT-Unternehmen trotz knapper Personalressourcen entschlossen sind, ihr Sicherheitsprofil zu verbessern. Abbildung 5 zeigt die wichtigsten Konzepte, die von den Verantwortlichen von Anlagenbetrieben auf die Frage genannt werden, welche Herausforderungen sie zur Verbesserung der Cyber-Sicherheit veranlassen.

Abbildung 5. Wichtige Herausforderungen treiben Erweiterungen bei Cyber-Sicherheit voran

Die Frage zu Abbildung 5 lautete: „Was sind die drei wichtigsten Herausforderungen, die Sie dazu veranlassen, Ihre Cyber-Sicherheitslage zu erweitern oder zu verändern?“ Je häufiger ein Begriff in den Antworten genannt wurde, desto größer ist er oben dargestellt.

Die häufigsten der von den Verantwortlichen für den Anlagenbetrieb genannten und in Abbildung 5 dargestellten Herausforderungen sind die Fähigkeit Hacker-Angriffe zu vereiteln, die durch die digitale Transformation erweiterte Angriffsfläche zu schützen, die Datensicherheit aufrechtzuerhalten und die Umgebungen sicher, produktiv, kosteneffizient und konform zu halten – und das alles bei einem Mangel an Fachkräften.

Erkenntnis: Bei OT-Unternehmen nimmt der Fokus auf Cyber-Sicherheit zu

70 % der befragten Unternehmen planen, OT-Cyber-Sicherheit im nächsten Jahr unter Leitung des CISO zu implementieren. Interessanterweise überwachen derzeit nur 9 % der CISOs die OT-Cyber-Sicherheit. In 50 % der Unternehmen ist derzeit der OT-Leiter/Manager der Cyber-Sicherheit für die Cyber-Sicherheit verantwortlich, weitere 24 % geben an, dass die Cyber-Sicherheit unter der Verantwortung des VP/Leiters von Netzwerktechnik und -betrieb steht.

Die Priorisierung der Cyber-Sicherheit zeigt sich nicht nur in der organisatorischen Umstrukturierung der Verantwortlichkeiten. **62 % der Unternehmen sagen, dass ihre Cyber-Sicherheitsbudgets** in diesem Jahr drastisch steigen, während 38 % ihre aktuellen Cyber-Sicherheitsbudgets beibehalten. OT-Unternehmen setzen Sicherheitsrisiken in den kritischen Fokus: 94 % der Befragten geben an, dass sie das OT-Sicherheitsprofil zu einem signifikanten oder moderaten Faktor der breiteren Risikobewertung machen, die der CISO der Geschäftsleitung und dem Vorstand weitergibt.

Erkenntnis: Der Schutz von OT-Umgebungen ist komplex

Die OT-Umgebungen, die von den Befragten geschützt werden müssen, sind komplex. Sie bestehen aus einer großen Anzahl von OT-Geräten, von weniger als 50 bis zu mehr als 500, wie in Abbildung 6 dargestellt.

Die meisten Unternehmen beziehen ihre Geräte von 2 bis 4 Anbietern, wie in Abbildung 7 dargestellt.

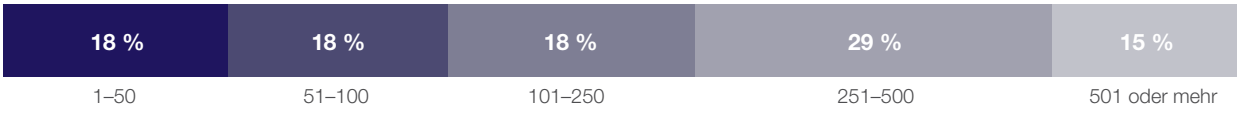


Abbildung 6. Anzahl der in Betrieb befindlichen OT-Geräte

Die am häufigsten genutzten OT-Anbieter in dieser Umfrage sind Honeywell, Siemens und Emerson, wie in Abbildung 8 dargestellt.

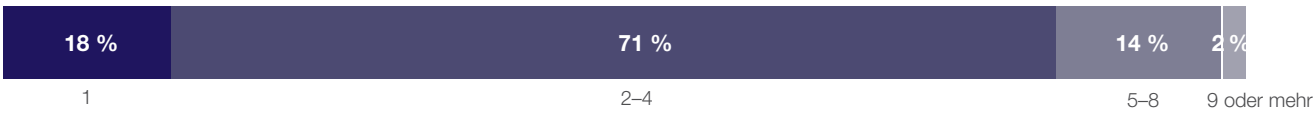


Abbildung 7. Anzahl der für OT-Geräte verwendete Anbieter

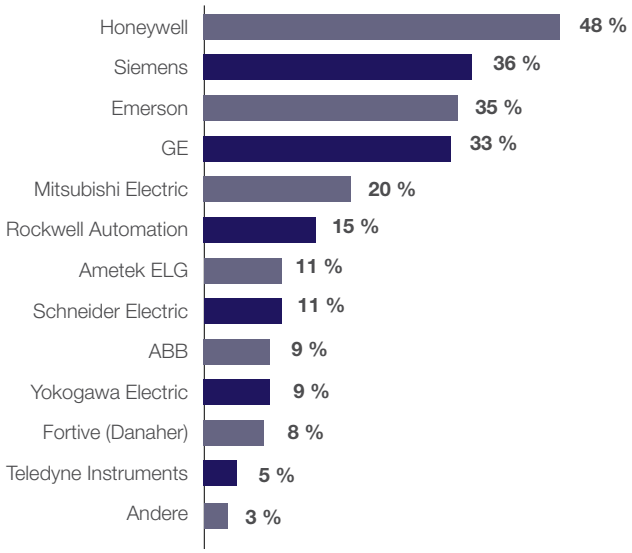


Abbildung 8. Für OT-Geräte verwendete Anbieter

Erkenntnis: Verantwortliche für den Anlagenbetrieb sind für die Verbesserung der Cyber-Sicherheit entscheidend

OT-Unternehmen stärken die Cyber-Sicherheit ihrer Umgebungen und die Verantwortlichen für den Anlagenbetrieb sind aktiv an den getroffenen Entscheidungen beteiligt. Mehr als drei Viertel (76 %) berichten, dass sie regelmäßig in Cyber-Sicherheitsentscheidungen einbezogen werden, und fast die Hälfte (45 %) hat bei OT-Entscheidungen das letzte Wort. Fast alle sind regelmäßig (56 %) oder gelegentlich (39 %) an der Entwicklung der IT-Cyber-Sicherheitsstrategie ihres Unternehmens beteiligt.

Es ist interessant festzustellen, dass ein sicheres und stabiles Umfeld für die drei wichtigsten Erfolgsmetriken, an denen die Verantwortlichen von Anlagenbetrieben gemessen werden, von wesentlicher Bedeutung ist: Maximierung der Produktivität (55 %), Minimierung der Kosten (53 %) und Reduzierung der Reaktionszeit bei Sicherheitsschwachstellen (44 %).

Es mag überraschen, dass die „Reduzierung der Reaktionszeit bei Sicherheitsschwachstellen“ die drittwichtigste Erfolgskennzahl ist. Dabei ist zu bedenken, wie schnell ein Cyber-Angriff Einrichtungen wie Fabriken, Versorgungsbetriebe oder Schienenverkehr stören und deren Produktivität, Ertrag und Sicherheit schaden kann. Ein stabiles und belastbares Umfeld ist auch für die drei wichtigsten unmittelbaren Verantwortungsbereiche der Verantwortlichen für den Anlagenbetrieb entscheidend: Bewerkstelligung der Produktionseffizienz (77 %), Überwachung des operativen Teams (77 %) und Bewerkstelligung der Qualitätskontrolle und der Fertigungsprozesse (76 %).

> ***„Die Bedrohung durch einen Cyber-Angriff belastet uns und wir investieren in die Prävention.“***
>
> – Betriebsleiter eines Produzenten

Angesichts ihres Fokus auf Stabilität und Belastbarkeit wird klar, warum 76 % der Verantwortlichen von Anlagenbetrieben aktiv in Cyber-Sicherheitsentscheidungen für OT-Systeme einbezogen werden. Diese Aufgabe wird mehr Zeit erfordern, da die Ausgaben für OT-Cyber-Sicherheit im Jahr 2023 voraussichtlich um 50 % auf 18,05 Milliarden USD steigen werden, gegenüber 12,22 Milliarden USD im Jahr 2017.[1]

Es gibt eine Reihe von Cyber-Sicherheitsmängeln, die OT-Teams angehen müssen, wie im nächsten Abschnitt erläutert.

Erkenntnis: OT-Sicherheitslücken sind in den Bereichen Zugriffskontrolle, Authentifizierung, Segmentierung, usw. vorhanden

Abbildung 9 zeigt den Prozentsatz der antwortenden OT-Unternehmen, die nicht über die folgend genannten wichtigsten Cyber-Sicherheitsfunktionen verfügen.

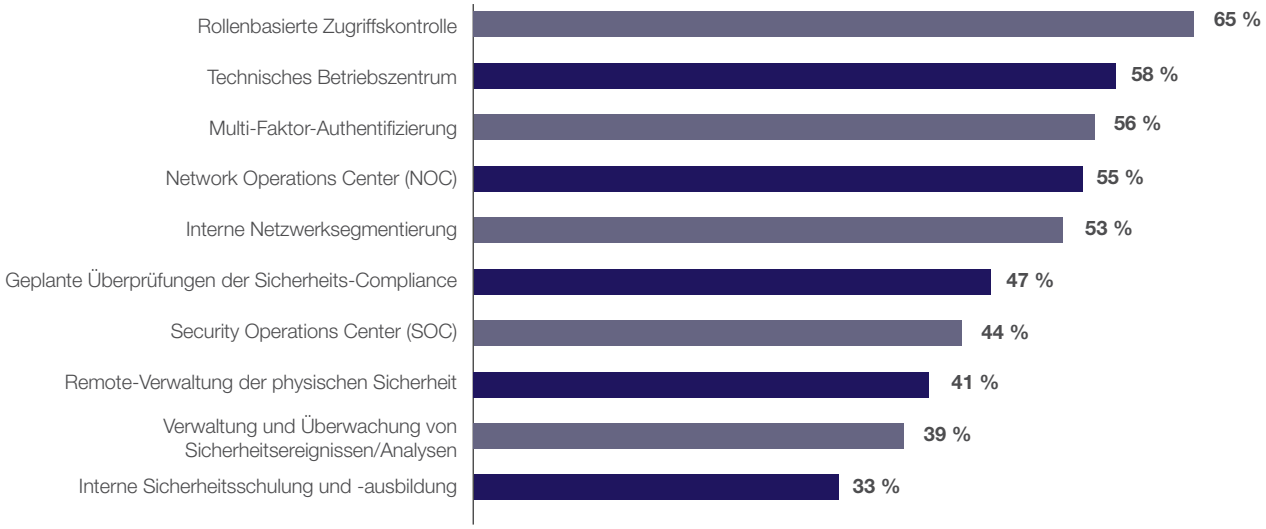


Abbildung 9. OT-Unternehmen, denen es an wichtigen Cyber-Sicherheits- und Security-Maßnahmen mangelt, in Prozent

Die fehlenden Fähigkeiten in Abbildung 9 führen zu einer Reihe von Sicherheitslücken:

- **Etwa zwei Drittel** (65 %) der befragten OT-Unternehmen verfügen nicht über eine rollenbasierte Zugriffskontrolle, was Angreifern mehr Bewegungsfreiheit innerhalb ihrer OT-Umgebungen gibt.
- **Fast 6 von 10** (56 %) OT-Unternehmen haben keine Multi-Faktor-Authentifizierung. Ein aktueller Verizon-Bericht stellt fest, dass 81 % der Datenschutzverletzungen auf verlorene oder gestohlene Zugangsdaten basieren.[2] Viele Datenschutzverletzungen in OT-Umgebungen gehen auf durch Spear-Phishing gestohlene Anmeldeinformationen zurück. (Schätzungsweise zwei Dutzend US-amerikanische Energieversorgungsunternehmen haben in den letzten zwei Jahren laut *Wall Street Journal* Speer-Phishing-Angriffe mit erfolgreichem Diebstahl von Zugangsdaten erlebt und Angreifer hinterließen Malware in ihren OT-Umgebungen, die für zukünftige Sabotage genutzt werden konnte.[3]) Die Multi-Faktor-Authentifizierung erschwert die erfolgreiche Verwendung gestohlener Anmeldeinformationen.
- **Mehr als die Hälfte** der Unternehmen (53 %) haben keine interne Netzwerksegmentierung. Die Cyber-Sicherheitsrichtlinien des National Institute of Standards and Technology (NIST) haben die Segmentierung als „eines der effektivsten Architekturkonzepte bezeichnet, die ein Unternehmen implementieren kann“, um seine OT-Umgebung zu schützen.[4] Branchenexperten weisen darauf hin, dass viele der jüngsten OT-Malware-Angriffe durch Segmentierung hätten verhindert werden können, da diese die Bewegungsfreiheit von Angreifern von einem OT-Produktionsnetzwerk zum anderen und sogar innerhalb eines OT-Produktionsnetzwerks einschränken.[5]
- **Fast die Hälfte** (44 %) verfügen über kein Security Operations Center (SOC) und mehr als die Hälfte (55 %) nicht über ein Network Operations Center (NOC), was zu einer geringeren Transparenz und einem erhöhten Risiko führt. Ein SOC kann eine Datenschutzverletzung schneller erkennen, vereiteln oder minimieren. Ein NOC maximiert den Netzwerkdurchsatz und die Verfügbarkeit. SOC und der NOC können integriert werden, um die Ergebnisse für beides zu verbessern.[6]
- **Fast 4 von 10 Unternehmen** (39 %) verwalten, überwachen oder analysieren keine Sicherheitsereignisse. Dies macht es schwierig, Datenschutzverletzungen aufzudecken. Da die meisten Unternehmen mittlerweile die Unvermeidlichkeit eines erfolgreichen unerlaubten Datenzugriffs erkannt haben, ist die Cyber-Resilienz – oder die Reaktion auf Datenschutzverletzungen und das Ereignismanagement – entscheidend, um die Auswirkungen einer Datenschutzverletzung zu minimieren.[7]
- Grundlegende Sicherheitspraktiken stellen für eine beträchtliche Anzahl von Unternehmen nach wie vor eine Herausforderung dar, wobei **ein Drittel** (33 %) zugibt, dass sie keine internen Security-Sensibilisierungsprogramme und -Schulungen haben. Da sich Insider-Bedrohungen für 30 % aller Verstöße verantwortlich zeichnen, sind solche Programme für jedes Unternehmen unbedingt erforderlich – IT ebenso wie OT.[8]

Best Practices von führenden OT-Security-Unternehmen

26 % unserer Befragten Unternehmem mit hervorragender OT-Security) („Top-Tier“) berichten von **keinerlei unbefugten Zugriffen** innerhalb der letzten 12 Monate. Andererseits erlebten 17 % unserer Befragten weniger geschützten OT-Unternehmen („Bottom-Tier“) in den letzten 12 Monaten **sechs oder mehr unbefugte Zugriffe**, und einige wussten nicht einmal, wie viele es tatsächlich waren. Es ist interessant, die Unterschiede zwischen diesen beiden Gruppen festzuhalten:

1. **„Top-Tier“-Unternehmen nutzen gegenüber den „Bottom-Tier“-Unternehmen zu 100 % Multi-Faktor-Authentifizierung,** die den Zugriff mit gestohlenen Zugangsdaten erschwert.

2. **„Top-Tier“-Unternehmen nutzen gegenüber den „Bottom-Tier“-Unternehmen zu 94 % rollenbasierte Zugriffskontrolle,** wodurch die Bewegung eines potenziellen Angreifers einschränkt wird.

3. **„Top-Tier“-Unternehmen verwalten und überwachen Sicherheitsereignisse gegenüber den „Bottom-Tier“-Unternehmen zu 68 % und führen Ereignisanalysen durch,** wodurch sie das von einer Datenschutzverletzung ausgehende Risiko verringern, da die Zeit bis zur Erkennung minimiert wird.

4. **„Top-Tier“-Unternehmen nutzen gegenüber den „Bottom-Tier“-Unternehmen zu 51 % Netzwerksegmentierung,** um die Bewegung eines potenziellen Angreifers einzuschränken.

5. **„Top-Tier“-Unternehmen planen gegenüber den „Bottom-Tier“-Unternehmen zu 46 % Überprüfungen der Sicherheits-Compliance** zur Stärkung des Sicherheitsprofils.

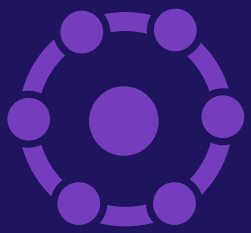
Fazit: Cyber-Sicherheit ist eine wachsende Anforderung für den Erfolg von OT

In OT-Umgebungen ist das Risiko hoch: Fast 8 von 10 erlebten im vergangenen Jahr Datenschutzverletzungen, die Hälfte berichtete von 3 bis 10 oder mehr. Es wurde von Datenschutzverletzungen berichtet, die sich auf Produktivität, Ertrag, Markenvertrauen, geistiges Eigentum und physische Sicherheit auswirkten. Diese Studie identifiziert Faktoren, die angegangen werden müssen, um Risiken zu reduzieren, wie z. B. die Tatsache, dass 78 % der Unternehmen keine vollständige, zentralisierte Sichtbarkeit der Cyber-Sicherheit haben, 56 % keine Multi-Faktor-Authentifizierung einsetzen und 53 % noch keine interne Netzwerksegmentierung verwenden, eine dringend empfohlenes Best Practice für OT-Umgebungen.[9]

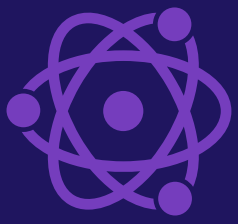
Die Verantwortlichen von OT-Anlagenbetrieben geben an, dass sie bei der Bewertung von Cyber-Sicherheitslösungen aktiv beteiligt sind. Sie suchen nach Lösungen, die ihre Hauptziele, die Maximierung der Produktivität bei gleichzeitiger Minimierung der Kosten, unterstützen.

Um dem Mangel an zentralisierter Transparenz und Sicherheitsexperten entgegenzuwirken, sollten OT-Unternehmen die folgenden Empfehlungen beachten:

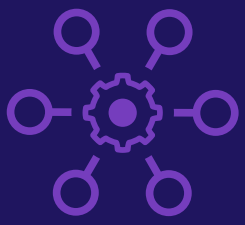
> ***„Security-Lösungen müssen intelligenter und effektiver agieren, und das häufig trotz knapperer Budgets.“***
>
> – VP Produktion einer großen Herstellerfirma



Suchen Sie nach Security-Lösungen, die zusammenarbeiten, um eine umfassende Sichtbarkeit der gesamten digitalen Angriffsfläche zu gewährleisten, die sich über OT- und IT-Umgebungen erstreckt.



Suchen Sie nach einem Security Fabric-basierten Ansatz, der integrierten Schutz über alle Geräte, Netzwerke und Anwendungen hinweg bietet.



Suchen Sie nach automatisierten Security-Funktionen und Lösungen, die Reaktionen koordinieren und Technologien wie maschinelles Lernen nutzen.

Minimieren Sie das Risiko mithilfe von Best Practices für die Cyber-Sicherheit in OT-Umgebungen wie Netzwerksegmentierung, Multi-Faktor-Authentifizierung und rollenbasierte Zugriffskontrolle.

Diese Cyber-Security-Ansätze verbessern das Sicherheitsprofil des Unternehmens und tragen gleichzeitig dazu bei, einen Mangel an qualifizierten Mitarbeitern auszugleichen.

Referenzen

[1] „Industrial Control Systems (ICS) Security Market worth $18.05 billion by 2023“, MarketsandMarkets, letzter Zugriff 25. Februar 2018.

[2] 2017 Data Breach Investigations Report, Verizon, letzter Zugriff 30. November 2018.

[3] Rebecca Smith and Rob Barry, „America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It“, The Wall Street Journal, 10. Januar 2019.

[4] Keith Stouffer, et al., „Guide to Industrial Control Systems (ICS) Security“, NIST, Mai 2015.

[5] Peter Newton, „Securing IIoT requires extra care. NAC and segmentation can help“, TechTarget, 28. September 2018.

[6] „Bridging the NOC-SOC Divide“, Fortinet, letzter Zugriff 5. März 2019.

[7] Patrick Spencer, „Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study“, Scalar Security Blog, 20. Februar 2019.

[8] „2018 Data Breach Investigations Report“, Verizon, März 2018.

[9] Keith Stouffer, et al., „Guide to Industrial Control Systems (ICS) Security“, NIST, Mai 2015.

FORTINET

www.fortinet.com

330327-0-1-DE

September 10, 2019 7:29 nachm.

E:\PRACE\ARGOS\2019\09 2019\A-344888-924139\de-DE\OT\Manufacturing-Plant Operations\report-state-of-operational-technology-A4_de-DE