FORTINET

BERICHT

COOs und Cyber-Security für Betriebstechnologie

Ein Bericht über aktuelle Prioritäten und Herausforderungen

Inhaltsverzeichnis

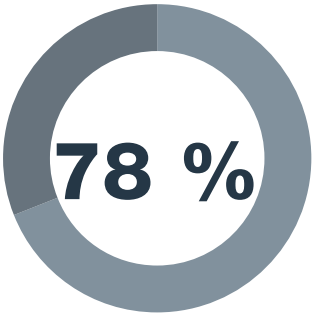
Zusammenfassung

Der Bericht „COOs und Cyber-Security für Betriebstechnologie“ von Fortinet untersucht die Herausforderungen, denen sich COOs bei der Sicherung von Betriebstechnologie-Infrastrukturen gegenübersehen, und wie COOs diese Probleme angehen. Obwohl die Verantwortung für die Sicherheit von Operational Technology (OT) normalerweise mit dem CISO oder einer anderen Führungskraft geteilt wird, spielen COOs bei der OT-Sicherheit eine zentrale Rolle, da ihre Teams häufig für das Management und den Kauf der in der Produktion verwendeten Geräte, Anlagen und Security-Tools verantwortlich sind.

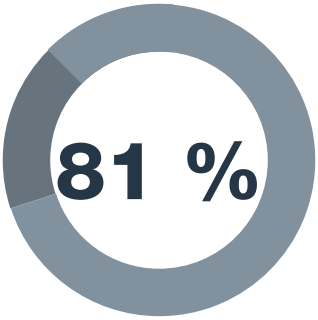
Eine aktuelle Fortinet-Umfrage ergab eine Reihe von Erkenntnissen über die Rolle des COO bei der OT-Sicherheit. Zu den wichtigsten Ergebnissen gehören:

1. Der COO steht vor einem **beispielloses Maß an Veränderung** infolge der Konvergenz von OT und IT, höheren Erwartungen von Führungskräften und einer zunehmenden Beteiligung des CISO an der Cyber-Sicherheit von Betriebstechnologie.
2. **Herausforderungen beim Risiko-Management** und die Frage, wie sich Sicherheitsprobleme lösen lassen, dominieren mittlerweile die tägliche Arbeit von COOs.
3. Führungskräfte sind bereit, das **Budget für die Cyber-Security von Betriebstechnologie (OT) zu erhöhen**, erwarten jedoch im Gegenzug, dass COOs mit diesen Investitionen greifbare Ergebnisse erzielen.
4. Weiter haben COOs angesichts der komplexen Bedrohungslage Schwierigkeiten, **mit Veränderungen Schritt zu halten**.

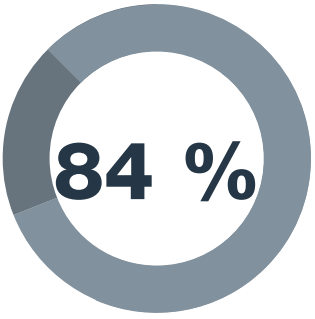
In Hinblick auf diese Entwicklungen und Herausforderungen haben wir die Daten eingehender analysiert und konnten anhand der Sicherheitsverletzungen im Vorjahr zwei Untergruppen von Befragten identifizieren: besonders erfolgreiche COOs und die COOs, die über die meisten Sicherheitsvorfälle berichteten. Anschließend analysierten wir die typischen Herangehensweisen der besonders erfolgreichen COOs und verglichen diese mit dem Vorgehen der schlecht abschneidenden Untergruppe. Dabei kristallisierten sich Best Practices heraus, die zeigen, dass erfolgreichere COOs die Cyber-Sicherheit und die betrieblichen Verantwortlichkeiten geschickt in Einklang bringen. Dazu gehören die Verfolgung und Vorlage von Cyber-Security-Kennzahlen, regelmäßige Überprüfungen der Sicherheit und Compliance sowie die Implementierung bewährter Sicherheitsmaßnahmen wie die Multi-Faktor-Authentifizierung.



sind direkt für die Einbettung der Sicherheit in betriebliche Prozesse verantwortlich

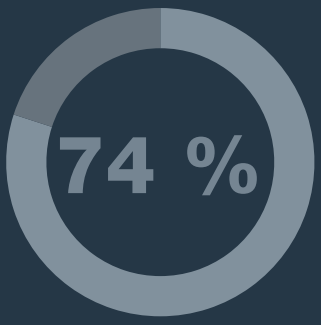


wirken regelmäßig an der Cyber-Security-Strategie des Unternehmens mit

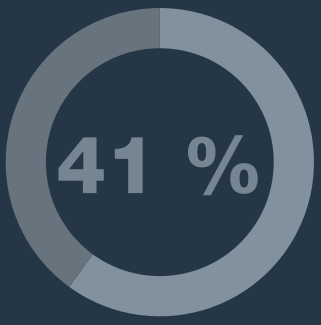


sind regelmäßig an Kaufentscheidungen für Cyber-Sicherheit beteiligt

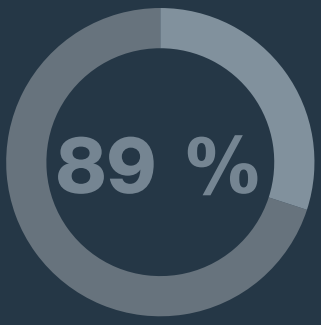
Infografik: Wichtigste Erkenntnisse



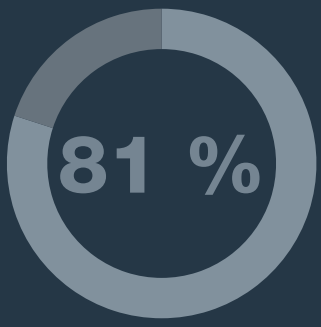
der Befragten verwalten mindestens 100 Geräte



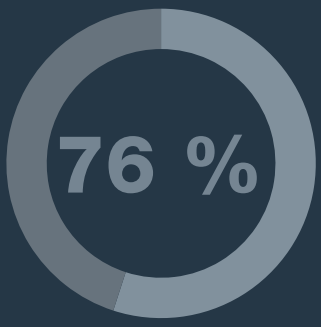
haben über 250 implementierte Geräte



verzeichneten in den letzten 12 Monaten einen Angriff



erlebten Ausfälle während Angriffen



erwarteten eine Erhöhung des Security-Budgets in 2019, wobei 1 von 10 Befragten von einer *erheblichen* Budget-Erhöhung ausging

Was erfolgreiche COOs auszeichnet:

168 % höhere Wahrscheinlichkeit, dass sie Änderungen der Compliance-Vorschriften als erfolgskritische Herausforderung betrachten

124 % höhere Wahrscheinlichkeit, dass sie in einem Unternehmen arbeiten, in dem die Cyber-Security dem leitenden Management untersteht

79 % höhere Wahrscheinlichkeit, dass sie die Produktionseffizienz zu den wichtigsten Erfolgskennzahlen zählen

45 % höhere Wahrscheinlichkeit, dass sie regelmäßige Compliance-Überprüfungen planen

Einleitung

Der Begriff „Betriebstechnologie (OT)“ bezieht sich auf die Infrastruktur, die Prozesse und Produktionsaktivitäten überwacht und steuert. Betriebstechnologie findet sich z. B. in Fertigungsanlagen, Stromnetzen, Wasserversorgungsunternehmen, in der Öl- und Gasförderung oder im Transportwesen. Früher arbeitete Betriebstechnologie nur mit Hard- und Software, die speziell für industrielle Anforderungen entwickelt wurde. Infolgedessen waren OT- und IT-Infrastrukturen in der Vergangenheit sowohl physisch als auch vom Management her voneinander getrennt.

Viele OT-Netzwerke sind nicht segmentiert und umfassen unterschiedlichste Produktionsprotokolle, unidentifizierte Ressourcen und ältere Geräte. Einige verwenden unsichere Kommunikationskanäle zu Unternehmens- und IT-Netzwerken, während andere gar keine Verbindung zum Internet und anderen externen Netzwerken haben. Der allgemeine Trend ist jedoch, dass sich Betriebstechnologie der „Außenwelt“ öffnet. Beispielsweise ergab eine aktuelle Umfrage, dass 34,5 % der Steuernetze mit dem Internet und 66,4 % entweder mit einer privaten Infrastruktur eines Drittanbieters oder mit deren Unternehmensnetzwerk verbunden sind.[1]

Die Zusammenführung von OT- und IT-Infrastrukturen liegt in der Industrie im Trend, da Unternehmen davon in vielerlei Hinsicht profitieren. Bei getrennten OT- und IT-Infrastrukturen ist der Datenaustausch ein komplizierter Prozess, der oft nur monatlich oder vierteljährlich erfolgt. Durch die Schaffung einer gemeinsamen Plattform für OT- und IT-Daten erhalten Unternehmen in Echtzeit Leistungsindikatoren (KPI), die auf aktuellen Informationen aus beiden Bereichen basieren. Solche Echtzeit-KPIs erlauben schnellere Reaktionen auf Marktveränderungen. Beispielsweise können Produktmanager auf einen plötzlichen Anstieg der Rohstoffkosten hingewiesen werden, der sich auf die Gewinnmargen auswirkt. IT- und OT-Manager profitieren gleichermaßen von der unternehmensweiten Transparenz und der Möglichkeit, trotz der Kluft zwischen IT und OT zusammenzuarbeiten.

Die Konvergenz von IT und OT hat jedoch erhebliche Auswirkungen auf die Sicherheit:

- **Erweiterte Angriffsfläche:** Bei einer vernetzten OT- und IT-Infrastruktur ist im Angriffsfall jeder Endpunkt in beiden Netzwerken gleichermaßen gefährdet. Relativ ungeschützte OT-Geräte wie Ventile, Pumpen, Sensoren, elektronische Schlösser, Thermostate und Roboter sind jetzt potenzielle Einstiegspunkte in die IT-Infrastruktur. Umgekehrt können Cyber-Kriminelle über das Mobilfunknetz in das IT-Netzwerk eindringen, um kritische Versorgungsunternehmen wie das Stromnetz oder Transportsysteme anzugreifen.
- **Erhöhte Komplexität:** Netzwerk-Umgebungen für Betriebstechnologie sind komplex. In der Regel müssen 50 bis 500 Geräte von verschiedenen Anbietern überwacht und gesichert werden. Diese Komplexität stellt höhere Herausforderungen an die Mitarbeiter und die Transparenz, da jedes Gerät seine eigenen Daten speichert, eine spezielle Sicherheitskonfiguration erfordert und unterschiedliche Anforderungen hat.
- **Komplexe Bedrohungslage:** Durch die Verbindung von Betriebstechnologie mit dem Internet wird die OT-Infrastruktur auch älterer Malware ausgesetzt. Während signaturbasierte IT-Sicherheitslösungen solche Malware leicht abfangen können, sind unzureichend geschützte Industriegeräte und -anlagen einer Gefährdung ausgesetzt. Cyber-Kriminelle testen häufig alte Malware, indem sie eine kleine Anzahl von Computern angreifen. Ist ein solcher Test-Exploit erfolgreich, werden Angriffe im großen Stil geplant. Durch dieses „Malware-Recycling“ können Cyber-Kriminelle den Wert existierender Schadsoftware maximieren, ohne in komplexe Attacken speziell gegen Betriebstechnologie investieren zu müssen.[2]

„Die Erweiterung der Angriffsfläche führt dazu, dass wir unsere Datenbank-Systeme besser schützen müssen.“

– Umfrageteilnehmer aus dem Energiesektor

„Die zunehmende Komplexität zwingt uns, mehr Zeit für die Cyber-Sicherheit aufzuwenden, was zu Lasten der Produktion geht.“

– Umfrageteilnehmer aus der Fertigungsindustrie

„Wegen der komplexen Bedrohungslage bringt das Team jede Woche viel mehr Stunden mit Security-Verbesserungen zu.“

– Umfrageteilnehmer aus dem Gesundheitswesen

Methodik dieser Studie

Der Bericht „Cyber-Security für Betriebstechnologie“ basiert auf einer Umfrage unter COOs. Befragt wurden Teilnehmer aus Unternehmen mit mehr als 2500 Mitarbeitern in verschiedenen Branchen, von denen über die Hälfte (59 %) im verarbeitenden Gewerbe und mehr als ein Viertel (27 %) im Energie- und Versorgungssektor tätig sind.

Anhand der Daten dieser Umfrage haben wir zuerst mehrere aktuelle Trends hinsichtlich der Rolle des COO bei der Sicherung der OT-Infrastruktur im Unternehmen identifiziert. Zudem haben wir die Antworten der Teilnehmer auf offene Fragen zu ihren wichtigsten Herausforderungen analysiert, um zu erfahren, inwiefern sich verschiedene Aspekte auf die tägliche Arbeit auswirken. Bei genauerer Untersuchung der Daten kristallisierte sich eine Untergruppe von Unternehmen heraus, die in den letzten 12 Monaten höchstens drei unbefugte Zugriffe erlebt hatte, sowie eine weitere Untergruppe, die im vergangenen Jahr über mindestens vier Sicherheitsverletzungen berichtete. Aus dem Vergleich dieser beiden Gruppen haben wir dann Best Practices für die Cyber-Sicherheit von Betriebstechnologie (OT) abgeleitet, die erfolgreiche COOs mit höherer Wahrscheinlichkeit befolgen.

Wichtige Entwicklungen bei der Cyber-Sicherheit von Betriebstechnologie für COOs

Trend: COOs sind für die Cyber-Sicherheit von Betriebstechnologie (OT) verantwortlich und haben Einfluss auf die Security-Strategie des Unternehmens.

Laut drei Viertel der Befragten ist der Unternehmensbereich für die Cyber-Sicherheit zuständig, in dem der COO arbeitet. Davon gaben 7 von 10 der Studienteilnehmer an, dass die OT-Cyber-Security dem OT-Leiter oder dem Manager für Cyber-Sicherheit unterstellt ist. Weitere 8 % nannten den VP oder den Leiter des Bereichs Netzwerk-Technik und -Betrieb als Verantwortliche (Abbildung 1). Die überwiegende Mehrheit (81 %) der COOs ist regelmäßig an der Ausarbeitung der Cyber-Security-Strategie beteiligt, während der Rest gelegentlich hinzugezogen wird (Abbildung 2).

Angesichts der Tatsache, dass OT und IT in vielen Unternehmen immer noch voneinander getrennt sind, ergibt es Sinn, dass der COO für die gesamte OT-Infrastruktur – einschließlich der Sicherheit – verantwortlich ist. Allerdings zeigt dieser Bericht, dass sich die Rolle des COO bei der Cyber-Security derzeit wandelt und dem COO immer mehr Verantwortung für Sicherheitsbelange zukommt.

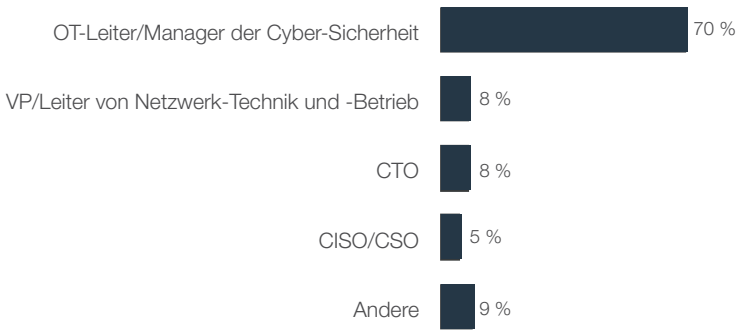


Abbildung 1: Zuständigkeit für die OT-Cyber-Security im Unternehmens

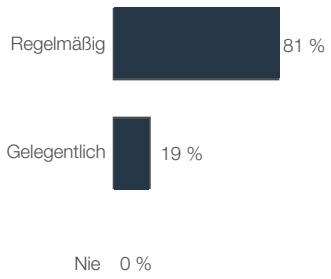


Abbildung 2: Beteiligung des COO an strategischen Cyber-Security-Entscheidungen

Trend: Das Sicherheitsmandat des COO ist innerhalb des Unternehmens gut sichtbar.

Es überrascht kaum, dass Unternehmen der OT-Sicherheit zunehmend Aufmerksamkeit schenken. Über die Hälfte (54 %) der COOs geben an, dass das OT-Sicherheitsprofil ein wichtiger Faktor für die Gesamtrisikobewertung des Unternehmens ist, während dies für mehr als ein Drittel (35 %) eine gewisse Rolle spielt (Abbildung 3). Das Risiko-Management dominiert dabei die Herausforderungen, denen sich COOs gegenübersehen. Dieses Thema wird im Folgenden unter „Zentrale Herausforderungen für COOs“ erörtert.

Der zunehmende Schwerpunkt auf die Sicherheit zeigt sich auch darin, dass COOs unterschiedlichste Security- und Compliance-Kennzahlen vorlegen müssen. Dazu gehören die Ergebnisse von Intrusion-Tests (70 %), Angaben zu Sicherheitsverletzungen (65 %), geplante Sicherheitsbewertungen (62 %) sowie die Einhaltung von Security-Standards und Branchenvorschriften (59 % bzw. 57 %) (Abbildung 4).

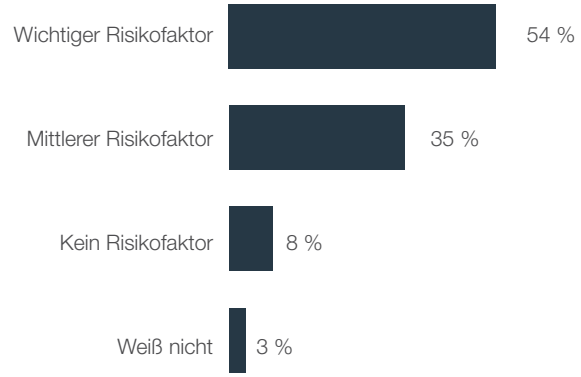


Abbildung 3: Einfluss des OT-Sicherheitsprofils auf die Einschätzung des Gesamtrisikos

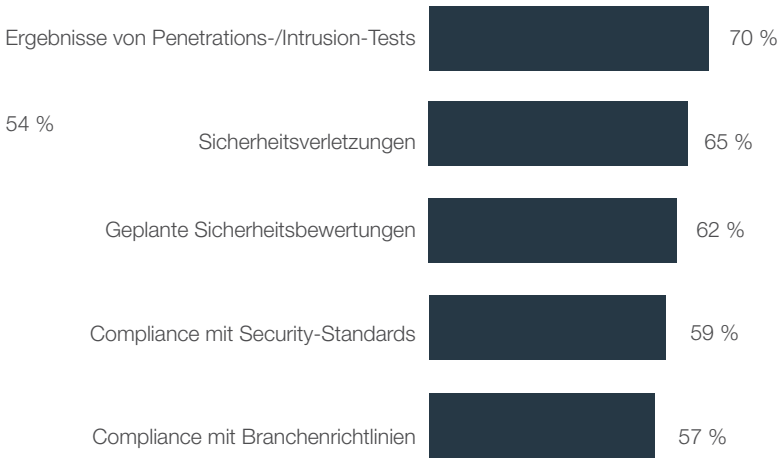


Abbildung 4: Bereiche, für die COOs Kennzahlen für die Cyber-Security von Betriebstechnologie (OT) vorlegen müssen

Trend: COOs tragen zusätzlich zum bisherigen operativen Schwerpunkt erhebliche Verantwortung für die Sicherheit.

Die Hauptaufgabe des COO besteht darin, reibungslose operative Abläufe sicherzustellen und die Betriebskosten unter Kontrolle zu halten. Über 8 von 10 Befragten sind direkt für das Erreichen der Produktionseffizienz (86 %), die Überwachung operativer Teams (86 %), das Auswählen und Verwalten der eingesetzten Betriebsmittel (86 %), die Leitung der Qualitätskontrolle (81 %) und die Überwachung von Technikern und Ingenieuren (81 %) zuständig. All diese Aufgabenbereiche fallen in die herkömmliche Rolle des COO: die Sicherstellung von reibungslosen Betriebsabläufen und die laufende Kontrolle der Betriebskosten.

Über diese Aufgaben hinaus erwarten Unternehmen, dass COOs mit dem CISO und anderen Security-Managern beim Schutz der Produktionsinfrastruktur zusammenarbeiten. Über drei Viertel (78 %) der Befragten geben an, für die Sicherung betrieblicher Prozesse verantwortlich zu sein – eine Aufgabe, für die viele COOs weder ausreichend geschult sind noch genug Erfahrung mitbringen (Abbildung 5). Ein wiederkehrendes Thema in diesem Bericht ist daher die Notwendigkeit für COOs, die wachsende Verantwortung bei der Security mit herkömmlichen operativen Aufgaben in Einklang zu bringen.

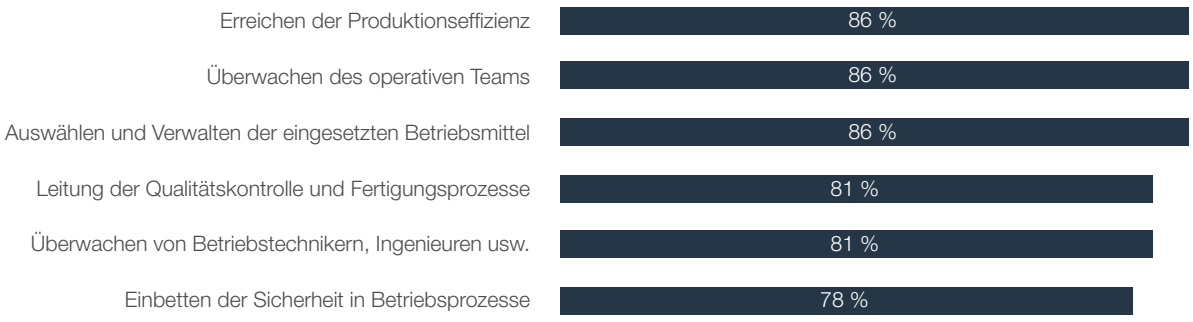


Abbildung 5: Direkte Zuständigkeiten von COOs

Trend: Die meisten COOs erlebten im vergangenen Jahr mehrere Sicherheitsverletzungen mit erheblichen Schäden für das Unternehmen.

Für die befragten COOs sind mehrfache Sicherheitsverletzungen leider die Regel und nicht die Ausnahme: Nur 11 % der COOs erlebten in den letzten 12 Monaten keine Angriffe. 42 % erlebten ein oder zwei Sicherheitsverstöße, während die restlichen 47 % mindestens drei Intrusionen verzeichneten (Abbildung 6). Die Art der Angriffe war recht unterschiedlich: 69 % hatten mit Malware und über 41 % mit Spyware- und Phishing-Angriffen zu kämpfen (Abbildung 7).

Von den Befragten, die bereits eine Sicherheitsverletzung erlebt hatten, berichteten 81 % von Ausfällen in der OT-Infrastruktur, die die Produktivität beeinträchtigten (53 %), die physische Sicherheit gefährdeten (31 %) oder zu Umsatzeinbußen führten (28 %). Im Gegensatz dazu ist die Häufigkeit von Schäden bei Angriffen auf die IT-Infrastruktur recht gering: Etwas mehr als ein Viertel (28 %) verlor geschäftskritische Daten und nur 22 % verzeichneten eine Verschlechterung des Marken-Images (Abbildung 8).

Im Vergleich dazu berichteten CISOs bei einer Fortinet-Studie, dass sich nur 40 % der Ausfälle auf die Produktivität, den Markenwert und Umsatz auswirkten.[3] Das schlechtere Abschneiden der Betriebstechnologie könnte jedoch auch andere Gründe haben – wie die höhere Transparenz bei der OT-Security oder die Einbeziehung des OT-Sicherheitsprofils in die allgemeine Risikobewertung. Diese Faktoren müssten bei der Interpretation anderer Ergebnisse in diesem Bericht berücksichtigt werden.

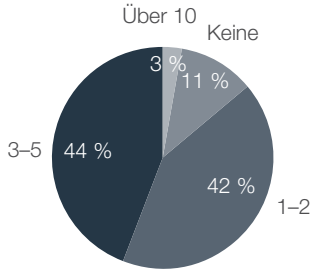


Abbildung 6: Anzahl der Sicherheitsverletzungen im vergangenen Jahr

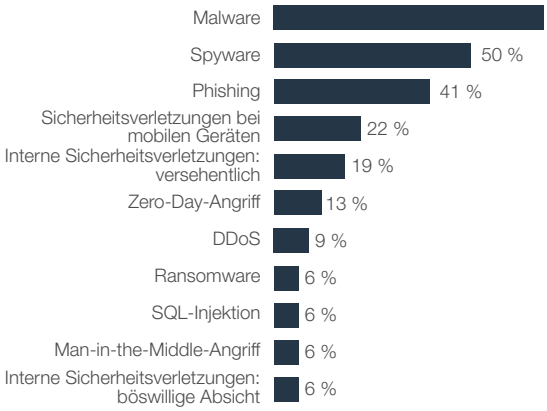


Abbildung 7: Art der erlebten Sicherheitsvorfälle

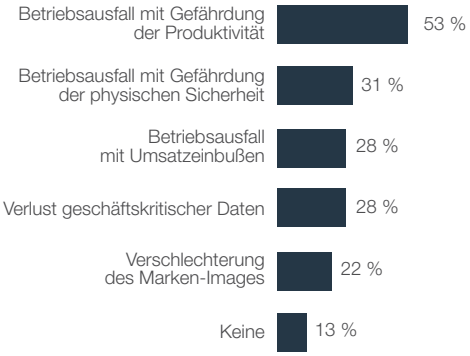


Abbildung 8: Auswirkungen von Sicherheitsverletzungen auf das Geschäft

Trend: Ausfälle können Erfolgskennzahlen von COOs beeinträchtigen.

Ausfälle können nicht nur das Geschäft schädigen, sondern auch einen direkten Einfluss auf die Karriere eines COO haben, da es schwieriger wird, bei Erfolgsmetriken gut zu punkten. Die fünf wichtigsten Erfolgsfaktoren für COOs sind die Kosteneffizienz (59 %), Produktivitätssteigerungen (54 %), die Sicherheitsbilanz (54 %), die Produktionseffizienz (51 %) und die Betriebszeit von Anlagen und Prozessen (30 %). All diese Metriken können durch ungeplante Ausfallzeiten negativ beeinflusst werden (Abbildung 9).

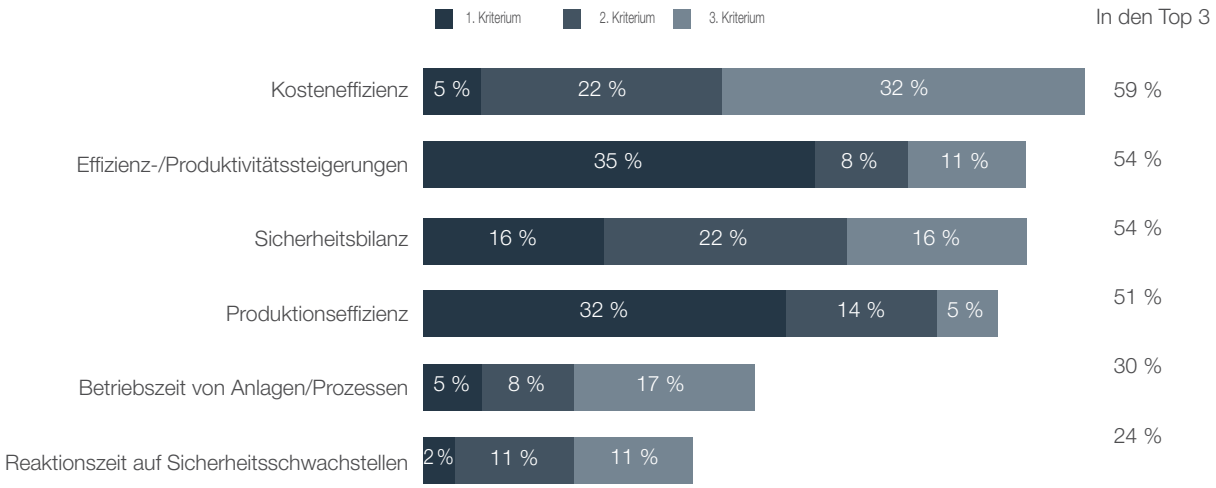


Abbildung 9: Erfolgsfaktoren für COOs

Trend: COOs erwarten – teilweise erhebliche – Erhöhungen bei Security-Budgets.

Ein weiteres Indiz für das zunehmende unternehmensweite Bewusstsein für die Risiken von Sicherheitsverletzungen in der OT-Infrastruktur ist die Bereitschaft des leitenden Managements, in die Sicherheit von Betriebstechnologie zu investieren. 76 % der COOs verzeichneten 2019 eine Erhöhung ihres Security-Budgets, wobei jeder Zehnte von einer *erheblichen* Budget-Erhöhung sprach (Abbildung 10). Eine andere Umfrage ergab, dass die OT-Budgets 2019 durchschnittlich um 17,9 % gestiegen sind.[4]

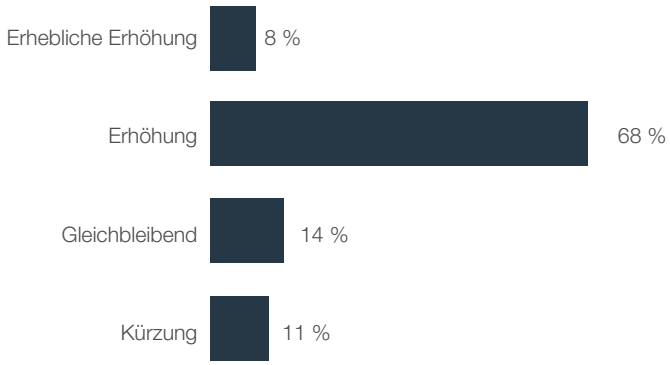


Abbildung 10: Entwicklung der Security-Budgets von COOs 2019

Genehmigt die Unternehmensleitung Investitionen in die Sicherheit, wird im Gegenzug erwartet, dass der COO weniger Sicherheitsverletzungen, Produktivitätssteigerungen und bessere Compliance-Bewertungen nachweisen kann. Entsprechend verfolgt und legt der Großteil der COOs Leistungskennzahlen für folgende Bereiche vor: Cyber-Security gegen Sicherheitsverletzungen (68 %), finanzielle Folgen (68 %), erkannte und blockierte Schwachstellen (62 %), Kostensenkung und Vermeidung von Ausgaben (57 %) und konkrete Ergebnisse beim Risiko-Management (51 %) (Abbildung 11). Weitere Informationen darüber, wie COOs auf Risiken reagieren, finden Sie im Abschnitt „Zentrale Herausforderungen für COOs“.

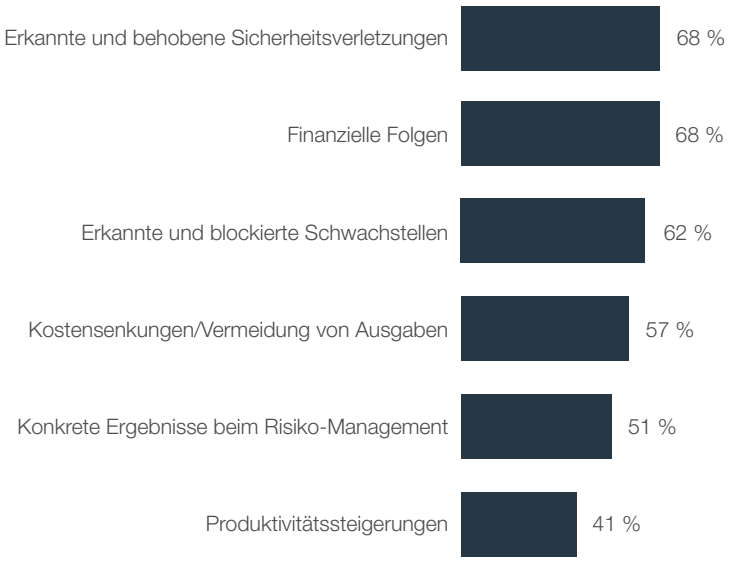


Abbildung 11: Erfasste und vorgelegte Cyber-Security-Kennzahlen

Trend: Die Rolle des COO befindet sich im Wandel, da die Hauptverantwortung für die OT-Sicherheit an den CISO verlagert wird.

Fast 9 von 10 Befragten (89 %) erwarten, dass der CISO im nächsten Jahr die Hauptverantwortung für die OT-Sicherheit übernimmt (Abbildung 12). Das liegt wahrscheinlich am Zusammenwachsen von Betriebstechnologie (OT) und Informationstechnologie (IT) und der Konsolidierung der Infrastruktur-Security, um das Sicherheitsprofil des gesamten Unternehmens zu stärken. Daher sollte diese Verlagerung nicht als Entlastung des COOs von der Cyber-Sicherheit interpretiert werden. Stattdessen wird dieser Aufgabenbereich voraussichtlich ausgeweitet, je mehr Maßnahmen zur Abwehr von Cyber-Angriffen im OT-Netzwerk hinzukommen. Auch das erwartete Wachstum bei der Anzahl intelligenter Industriegeräte dürfte den COO bei der Security noch stärker unter Druck setzen.

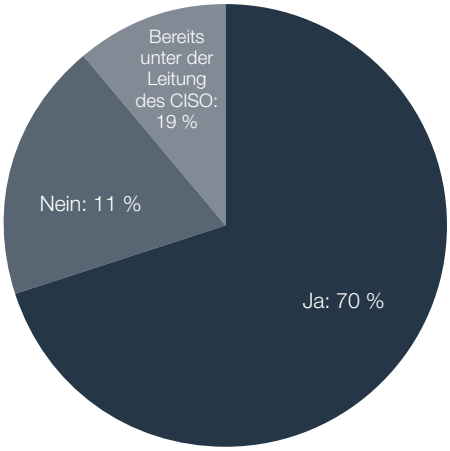


Abbildung 12: Verlagerung der OT-Cyber-Security an den CISO innerhalb eines Jahres

Trend: COOs verfolgen und legen mit höherer Wahrscheinlichkeit als CISOs wichtige Kennzahlen zur Cyber-Security vor.

Wie bereits erwähnt, werden CISOs in den meisten Unternehmen bald die Hauptverantwortung für die OT-Sicherheit übernehmen. Dieser Trend bedeutet, dass CISOs und COOs in Fragen der OT-Cyber-Sicherheit zusammenarbeiten müssen – was für beide Neuland ist. Vergleicht man die Tendenzen bei CISOs und COOs bei der Messung und Vorlage von Cyber-Sicherheitsmetriken, zeigen sich einige interessante Ähnlichkeiten und Unterschiede.

Zunächst verfolgen COOs weitaus häufiger als CISOs die vier wichtigsten Kennzahlen zur Cyber-Sicherheit: erkannte und behobene Sicherheitsverletzungen (68 % gegenüber 59 %), finanzielle Folgen (68 % gegenüber 46 %), gefundene und blockierte Schwachstellen (62 % gegenüber 44 %) und Kostensenkung/Vermeidung von Ausgaben (57 % gegenüber 51 %) (Abbildung 13). Diese Unterschiede ergeben Sinn vor dem Hintergrund, dass die Hauptverantwortung des COO das Management von Produktionsprozessen umfasst, die per se datengesteuert sind. CISOs im OT-Bereich tun daher gut daran, hier den Kriterien der COOs zu folgen, um die allgemeine Wirksamkeit von Sicherheitsinitiativen zu messen. Dieser Ansatz dürfte auch die Kommunikation mit der Unternehmensleitung wie dem CEO oder CFO sowie mit dem Vorstand effektiver gestalten.[5]

Der größte Unterschied zeigt sich bei der Erfassung der finanziellen Folgen, die über zwei Drittel (68 %) der COOs, aber nur weniger als die Hälfte (46 %) der CISOs praktizieren. Dieses Ergebnis spiegelt wahrscheinlich die Bedeutung wider, die Unternehmen den Gewinnmargen beimessen, die stark von Faktoren im Zuständigkeitsbereich des COO beeinflusst werden. Angesichts der Tatsache, dass COOs häufig mehr Erfahrung mit der Verfolgung finanzieller Auswirkungen haben, sollten CISOs die Gelegenheit nutzen, die Best Practices ihrer Kollegen zu übernehmen und finanzielle Aspekte stärker in den Vordergrund zu rücken.

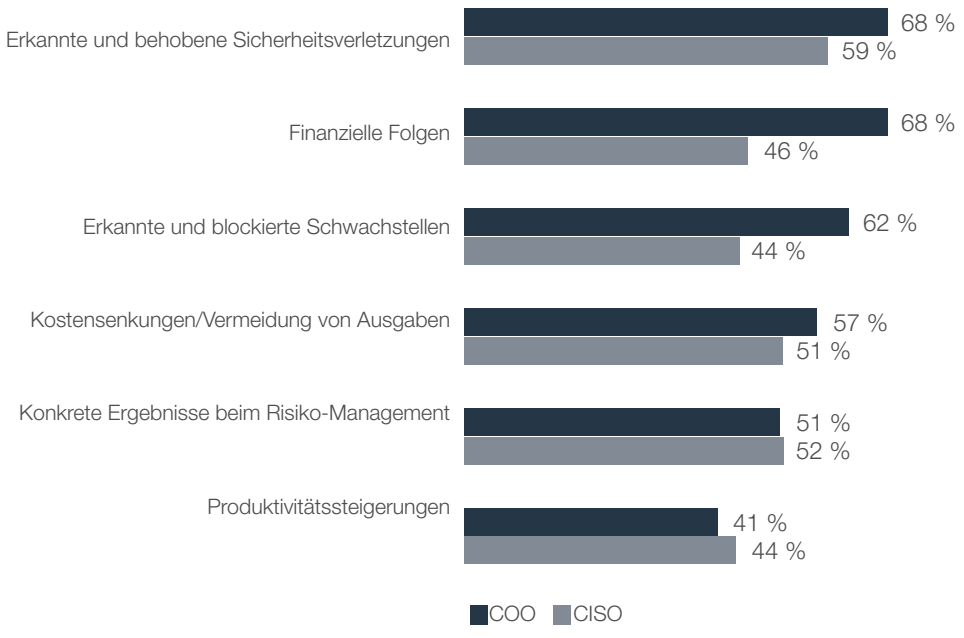


Abbildung 13: Vergleich von COOs und CISOs bei erfassten und vorgelegten Kennzahlen

Trend: COOs müssen bei Kaufentscheidungen für Cyber-Sicherheitslösungen die Komplexität berücksichtigen.

Die überwiegende Mehrheit (84 %) der COOs ist regelmäßig an Kaufentscheidungen für die OT-Cyber-Sicherheit beteiligt, während der Rest (16 %) gelegentlich hinzugezogen wird (Abbildung 14). COOs berichten, dass diese Entscheidungen negative Auswirkungen auf die Komplexität (70 %), die Einführung von Sicherheitsstandards (54 %) und die betriebliche Effizienz (49 %) haben können (Abbildung 15). Wie in vielen anderen Bereichen muss der COO bei Kaufentscheidungen die Notwendigkeit von Sicherheitsmaßnahmen mit der betrieblichen Effizienz in Einklang bringen. Die Folgen von Komplexität auf das Gesamtrisiko eines Unternehmens werden im Abschnitt „Zentrale Herausforderungen für COOs“ besprochen.

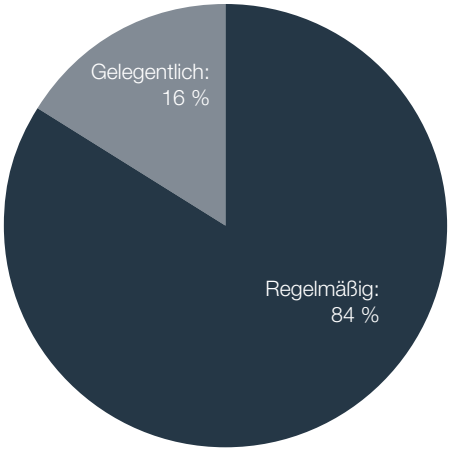


Abbildung 14: Beteiligung des COO an Kaufentscheidungen für Betriebstechnologie (OT)

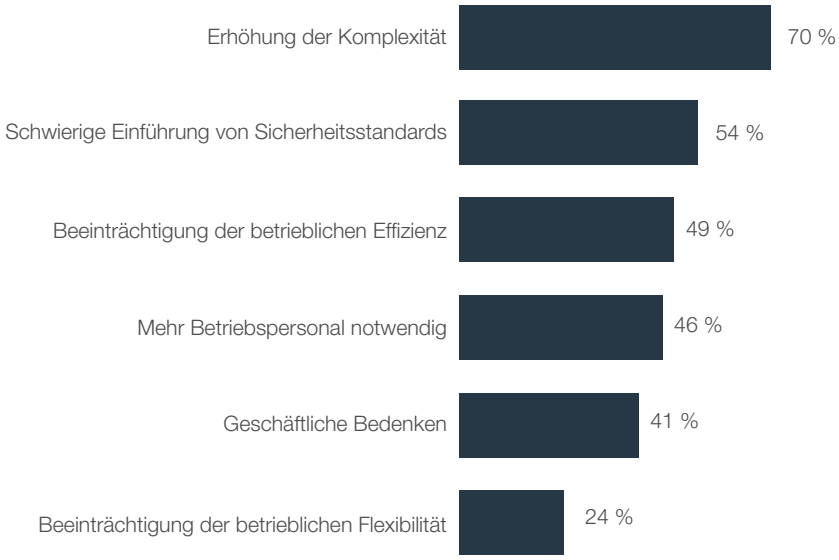


Abbildung 15: Wie sich Cyber-Security-Lösungen negativ auf den beruflichen Erfolg von COOs auswirken.

Zentrale Herausforderungen für COOs

Bei unserer Umfrage stellten wir auch einige offene Fragen zu den wichtigsten Herausforderungen von COOs im beruflichen Alltag. Obwohl die Antworten sehr unterschiedlich ausfielen, haben wir sie in Kategorien eingeteilt, um ein Gefühl dafür zu bekommen, was für COOs im Hinblick auf die Betriebstechnologie (OT) am wichtigsten ist. Im Mittelpunkt unserer Fragen standen die Herausforderungen, die sich aus drei wichtigen Sicherheitstrends ergeben: der komplexen Bedrohungslage, der Erweiterung der Angriffsfläche und der erhöhten Komplexität.

Herausforderung: Die Mehrheit der COOs nennt „Schritt halten mit Veränderungen“ als große Herausforderung angesichts der komplexen Bedrohungslage.

Gleich nach dem Risiko-Management als größte Herausforderung geben 61 % der COOs an, dass sie angesichts der komplexen Bedrohungslage nur schwer mit Veränderungen Schritt halten können (Abbildung 17). Dieses Ergebnis lässt sich dadurch erklären, dass viele Unternehmen die ehemals isolierte OT-Infrastruktur zunehmend mit der Außenwelt vernetzen. Infolgedessen wird die OT-Infrastruktur plötzlich massiv mit älterer Malware bombardiert. Solche veralteten Exploits stellen eine geringe Bedrohung für die IT-Infrastruktur dar, können jedoch in bestimmten Bereichen eines OT-Systems, in denen es keinen signaturbasierten Schutz gibt, zu Chaos führen. Daher ist es nicht verwunderlich, dass COOs Probleme haben, mit diesen neuen Herausforderungen Schritt zu halten.

Herausforderung: Die wachsende Angriffsfläche erschwert es COOs, Risiken zu erkennen und zu kontrollieren, mit Veränderungen Schritt zu halten und illegale Zugriffe zu verhindern.

Laut den befragten COOs erschwert die wachsende Angriffsfläche das Risiko-Management (65 %), das Schritthalten mit Veränderungen (48 %) und das Ergreifen von Abwehrmaßnahmen (26 %) (Abbildung 18). Mit Veränderungen Schritt zu halten ist ein wiederkehrendes Thema in diesem Teil der Umfrage, das in allen drei Bereichen den zweiten Platz belegt.

Herausforderung: Die zunehmende Komplexität des Cyber-Security-Managements trägt wesentlich zur Arbeitsbelastung und zum Berufsstress von COOs bei.

OT-Netzwerke werden allein durch die Anzahl der eingesetzten Geräte immer komplexer. Von den Befragten müssen 87 % mindestens 100 Geräte und 41 % sogar über 250 Geräte verwalten (Abbildung 16). Diese steigenden Gerätezahlen tragen zur Komplexität bei, insbesondere im Hinblick auf Updates und Wartungen.

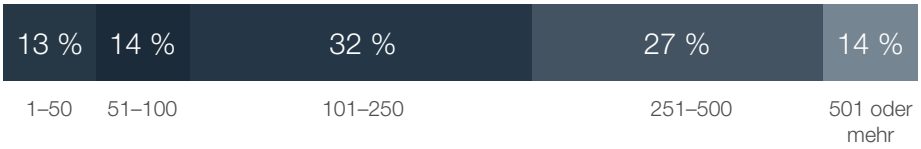


Abbildung 16: Anzahl der eingesetzten OT-Geräte

„Was Cyber-Security-Verantwortliche und Führungskräfte stark beunruhigt, ist die ständig wachsende Angriffsfläche, mit der sie jeden Tag erneut konfrontiert sind.“

– Diskussionsteilnehmer beim National Cyber Security Alliance Summit[6]

Fast ein Drittel (32 %) der Befragten gibt an, dass durch das komplexe Management von Cyber-Sicherheitssystemen ihre Arbeitslast und damit ihr Stresspegel gestiegen ist. Fast ebenso viele (29 %) geben an, dass sich wegen dieser Komplexität auch die Qualifikationslücke schwerer schließen lässt – wodurch COOs weiter unter Druck geraten, was wiederum zu einer erhöhten Arbeitsbelastung und beruflichem Stress (32 %) beiträgt (Abbildung 19).

Diese Erkenntnis impliziert, dass COOs vor großen Herausforderungen stehen, ihre Zuständigkeit für die OT-Cyber-Security mit anderen Aufgaben wie der Sicherung der Verfügbarkeit, Effizienz und Produktivität in Einklang zu bringen. Dieser Trend dürfte sich noch verstärken, wenn die Anzahl der OT-Geräte und die Komplexität des Geräte-Managements weiter zunehmen.

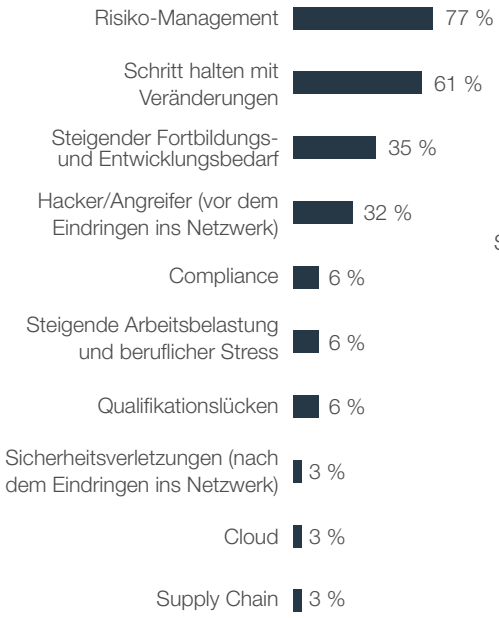


Abbildung 17: Herausforderungen für COOs aufgrund der komplexen Bedrohungslage

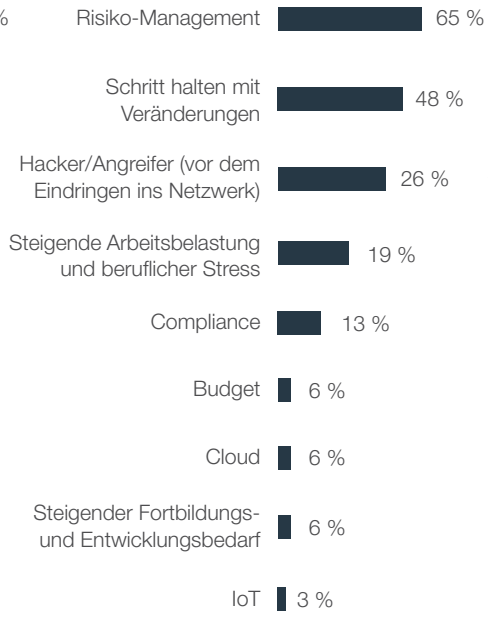


Abbildung 18: Herausforderungen für COOs aufgrund der erweiterten Angriffsfläche

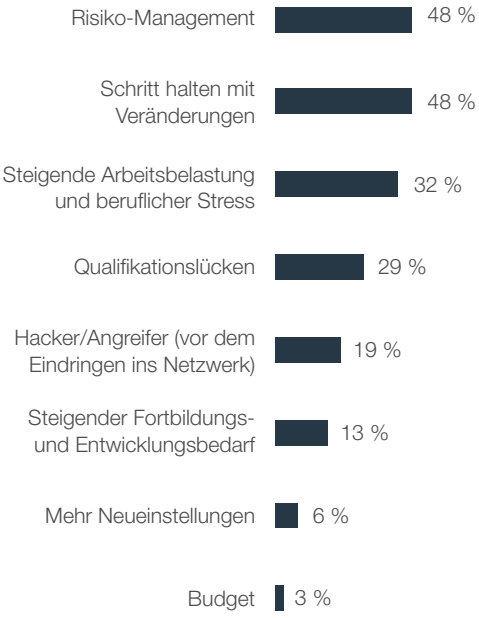


Abbildung 19: Herausforderungen für COOs aufgrund erhöhter Komplexität

Herausforderung: Insgesamt ist das Risiko-Management die größte Herausforderung für die Cyber-Sicherheit, mit der heutige COOs konfrontiert sind.

Die Gefahr durch Angriffe ist heute das Hauptanliegen von Unternehmen jeder Größe: Von 1200 Führungskräften gaben 55 % bei einer kürzlich durchgeführten Umfrage an, dass ihnen Bedrohungen durch Cyber-Attacken eine gewisse oder größere Sorge bereiten.[7]

Insgesamt wurde in diesem Teil der Umfrage das Risiko-Management häufiger als jeder andere Faktor genannt. 77 % führen Probleme mit dem Risiko-Management auf die komplexere Bedrohungslage zurück (Abbildung 17), 65 % auf die erweiterte Angriffsfläche (Abbildung 18) und 48 % auf die erhöhte Komplexität (Abbildung 19). Dieses Ergebnis steht im Einklang mit der zuvor gewonnenen Erkenntnis, dass das OT-Sicherheitsprofil die allgemeine Risikobewertung des Unternehmens beeinflusst.

Um zusätzlichen Kontext bereitzustellen, haben wir die COO-Ergebnisse mit den Umfrageergebnissen bei CIOs,[8] CISOs[9] und Netzwerk-Verantwortlichen[10] verglichen (Abbildung 20). Dabei fallen mehrere Punkte ins Auge:

„Wegen der erhöhten Komplexität werden unsere Mitarbeiter darin geschult, neue Technologien proaktiv anzuwenden.“

– Umfrageteilnehmer aus dem Energiesektor

- Im Vergleich zu CIOs, CISOs und Netzwerk-Verantwortlichen betrachten mehr COOs die immer komplexere Bedrohungslage als Herausforderung für das Risiko-Management. Eine positive Interpretation dieses Befundes ist, dass COOs sich der Herausforderungen bewusst sind, die sich aus der relativ unsicheren OT-Infrastruktur ergeben, und diese Realität richtigerweise als Risiko für das Unternehmen erkennen.
- Gegenüber CIOs und CISOs bewerten weit mehr COOs und Netzwerk-Verantwortliche das Risiko-Management als größte Herausforderung im Bereich Cyber-Sicherheit. Dieses Ergebnis bedeutet aber nicht, dass sich CIOs und CISOs nicht um das Risiko-Management kümmern, sondern es spiegelt vielmehr deren Prioritäten wider. Beispielsweise betrachten sowohl CIOs als auch CISOs den steigenden Fortbildungs- und Entwicklungsbedarf als eine größere Herausforderung als das Risiko-Management.
- CIOs bezeichnen das Risiko-Management am seltensten als größte Herausforderung bei der Cyber-Security. Dieses Ergebnis könnte auf die Tatsache zurückgehen, dass sich CIOs eher auf die Verfügbarkeit und Zuverlässigkeit als auf die Sicherheit konzentrieren. Eine weitere mögliche Erklärung ist, dass ein CIO einfach mehr Erfahrung im Risiko-Management hat und daher Faktoren wie die wachsende Angriffsfläche weniger wahrscheinlich als großes Hindernis für ein angemessenes Risiko-Management betrachtet.

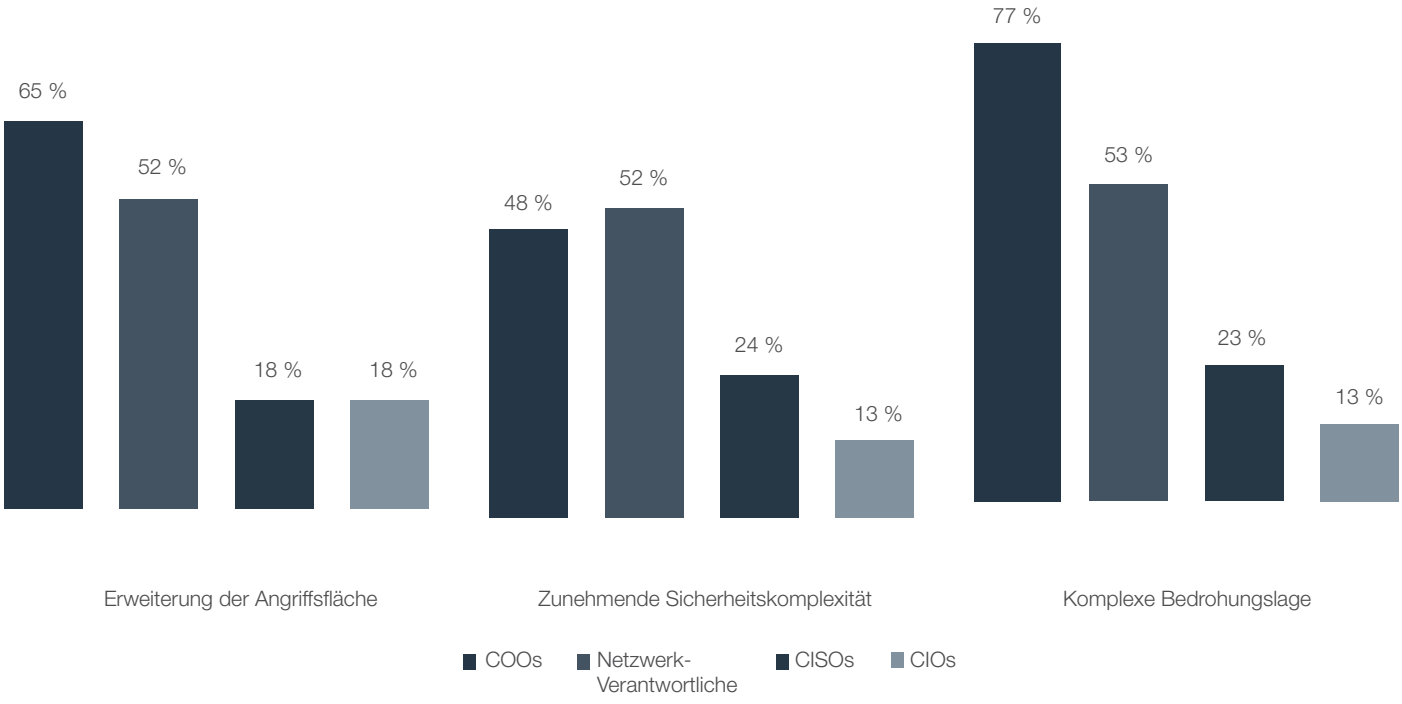


Abbildung 20: Prozentsatz der Befragten, die Herausforderungen beim Risiko-Management anführen: COOs, IT-Leitern und CISOs im Vergleich

Best Practices erfolgreicher COOs

Wir haben die Antworten aus zwei Untergruppen – die mit der besten und die mit der schlechtesten Bilanz bei Sicherheitsverletzungen – verglichen. Diese Analyse ergab eine Reihe von Best Practices, die erfolgreiche COOs wahrscheinlich häufiger anwenden:

1. Erfolgreiche COOs betrachten Änderungen der Compliance-Vorschriften mit einer höheren Wahrscheinlichkeit von 168 % als erfolgskritische Herausforderung und planen daher mit 45 % höherer Wahrscheinlichkeit regelmäßige Compliance-Überprüfungen ein.

Während die Befragten mehrere Probleme nannte, die sich auf ihre Arbeit auswirken, gaben die erfolgreichsten COOs mit einer höheren Wahrscheinlichkeit von über 168 % regulatorische Änderungen als eine der drei größten Herausforderungen für ihren beruflichen Erfolg an. Damit steht auch folgendes Ergebnis in Zusammenhang: Erfolgreiche COOs führen mit einer um 45 % höheren Wahrscheinlichkeit regelmäßige Compliance-Überprüfungen der Sicherheitsmaßnahmen durch. Dies ist ein wahrscheinlicher Indikator dafür, dass diese COOs proaktiv auf regulatorische Herausforderungen reagieren.

2. Erfolgreiche COOs arbeiten mit 124 % höherer Wahrscheinlichkeit in einem Unternehmen, in dem die Cyber-Security dem leitenden Management untersteht.

Angesichts des zuvor diskutierten gestiegenen Bewusstseins für die Wichtigkeit der OT-Sicherheit im Unternehmen überrascht es kaum, dass eine Zuständigkeit auf oberster Führungsebene mit weniger Angriffen korreliert. Wie bereits erwähnt, verlagern viele Unternehmen die Verantwortung für die OT-Cyber-Security an den CISO, was sich in weniger Sicherheitsverletzungen zeigen sollte.

3. Erfolgreiche COOs zählen mit 79 % höherer Wahrscheinlichkeit die Produktionseffizienz zu den wichtigsten Erfolgskennzahlen.

COOs vollbringen ständig einen Balance-Akt zwischen ihrem bisherigen betrieblichen Schwerpunkt und steigenden Erwartungen an die Security der OT-Infrastruktur. Erfolgreiche COOs finden Wege, um Sicherheitsverpflichtungen zu erfüllen und sich weiterhin auf die betriebliche Effizienz zu konzentrieren.

4. Erfolgreiche COOs setzen mit 49 % höherer Wahrscheinlichkeit eine Multi-Faktor-Authentifizierung ein.

Die Multi-Faktor-Authentifizierung ist eine bewährte Methode, um das Sicherheitsprofil eines Unternehmens zu verbessern. Laut einer Studie ist die Ergänzung von Passwörtern um eine Multi-Faktor-Authentifizierung unter Security-Experten die mit Abstand häufigste Schutzmaßnahme auf individueller Ebene.[11] Diese bewährte Methode haben erfolgreiche COOs für die Cyber-Security übernommen, wodurch die Bedrohungsabwehr zusätzlich gestärkt wird.

5. Erfolgreiche COOs erfassen mit 34 % höherer Wahrscheinlichkeit Produktivitätssteigerungen als Kennzahl für die Cyber-Security.

Die Produktivität ist bei COOs das Erfolgskriterium Nr. 1. Daher ist es sinnvoll, Security-Programme an die betriebliche Effizienz zu knüpfen, z. B. um durch Automatisierung Aufgaben schneller zu erledigen oder um manuelle Betriebsabläufe zu vermeiden. Erfolgreiche COOs verfolgen mit 49 % höherer Wahrscheinlichkeit die finanziellen Folgen als Cyber-Security-Kennzahl.

Unternehmen bewerten COOs routinemäßig anhand der finanziellen Gesamtleistung. Es überrascht daher kaum, dass erfolgreiche COOs ihren Prozess zur Budget-Verfolgung auf Verantwortlichkeiten im Bereich Cyber-Security ausweiten.

6. Erfolgreiche COOs legen mit 34 % höherer Wahrscheinlichkeit die Ergebnisse von Penetrations- und Intrusion-Tests dem Zuständigen für die Cyber-Security vor.

Dieses Ergebnis unterstreicht die Bedeutung, die Cyber-Security-Verantwortliche Tests beimessen, um eine möglichst genaue Risikobewertung zu erhalten. Proaktives Testen offenbart Schwachstellen und zeigt den Handlungsbedarf bei Sicherheitslücken auf. Dass erfolgreiche COOs Zeit für Tests haben, deutet darauf hin, dass sie für tägliche Routine-Aufgaben über zusätzliches Security-Personal verfügen.

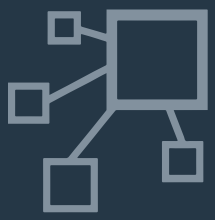
Fazit

Die Studie zeigt, dass die Arbeit von COOs in Bezug auf die OT-Cyber-Sicherheit im Unternehmen gut sichtbar ist. Auch sind COOs stark gefordert, Risiken zu managen und ihre Verantwortung für die Cyber-Security zusätzlich zu ihren herkömmlichen operativen Aufgaben wahrzunehmen. COOs, die ihre Security-Performance verbessern möchten, können folgende Best Practices von erfolgreicheren Kollegen übernehmen:

Reporting und Verfolgung wichtiger Security- und Betriebskennzahlen

Durchführung regelmäßiger Sicherheitstests und Compliance-Prüfungen

Schwerpunkt auf die finanziellen Folgen der Cyber-Security



Investition in bewährte Schutzmaßnahmen wie die Multi-Faktor-Authentifizierung

Referenzen

[1] Barbara Filkins und Doug Wylie: „SANS 2019 State of OT/ICS Cybersecurity Survey“. SANS Institute, 11. Juni 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] „The CISO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 26. April 2019.

[4] Barbara Filkins und Doug Wylie: „SANS 2019 State of OT/ICS Cybersecurity Survey“. SANS Institute, 11. Juni 2019.

[5] „The CFO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 11. September 2019.

[6] Doug Olenick: „Expanding Attack Surfaces and Difficulties Obtaining The Right People Worry NCSA panelists“. SC Magazine, 16. Oktober 2018.

[7] „Cyber Risk Is Top Concern for All, SMB Risks CISOs Need to Heed“. The CISO Collective, 25. Oktober 2019.

[8] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[9] „The CISO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 26. April 2019.

[10] „Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges“. Fortinet, 4. September 2019.

[11] „The 2019 State of Password and Authentication Security Behaviors Report“. Ponemon Institute, Januar 2019.

FORTINET

www.fortinet.com/de

4. Januar 2020, 4:13 Uhr

323524-0-1-DE