BERICHT

Bericht zum Stand der Betriebstechnologie (OT) und Cybersecurity 2023

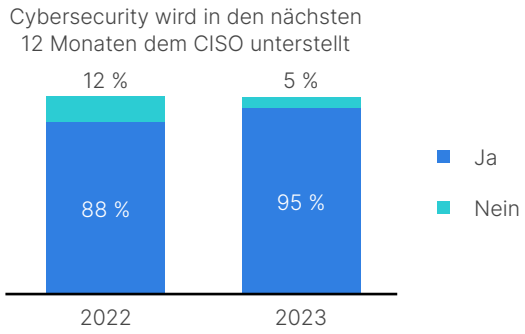
FORTINET

Inhalt

Wichtigste Ergebnisse

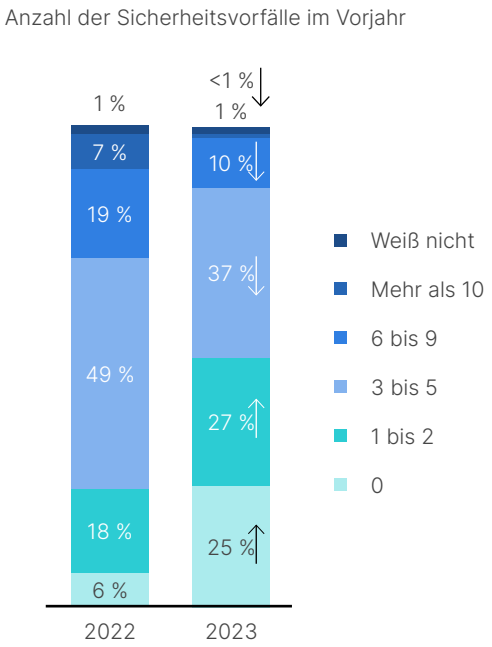
OT-Sicherheitsexperten

In fast allen befragten Unternehmen ist der CISO jetzt (oder demnächst) für die OT-Cybersecurity verantwortlich und immer mehr OT-Cybersicherheitsexperten stammen aus leitenden Funktionen der IT-Security, nicht mehr aus dem Operations-Team.



Cybersecurity-Vorfälle

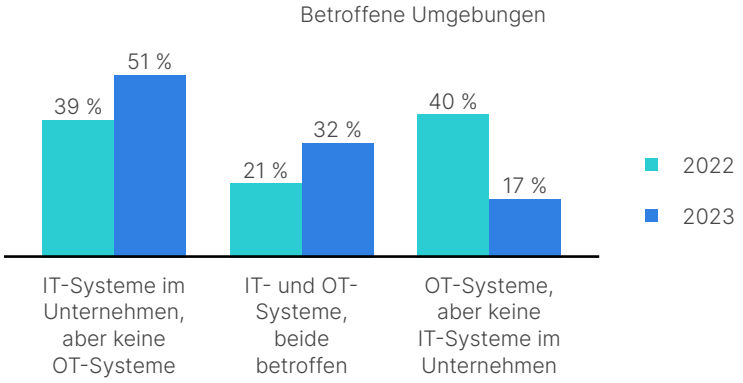
Während gegenüber dem Vorjahr erheblich mehr Unternehmen von Cyberangriffen verschont blieben (nur 6 % in 2022, dagegen **25 % in 2023**), gibt es weiterhin viel Verbesserungspotenzial. Tatsächlich meldeten drei Viertel der OT-Unternehmen mindestens einen illegalen Zugriff im letzten Jahr. Und fast ein Drittel der Befragten gab an, Opfer eines Ransomware-Angriffs geworden zu sein (**32 %**, unverändert gegenüber 2022). Insbesondere Sicherheitsvorfälle durch Malware und Phishing nahmen um **12 %** bzw. **9 %** zu.



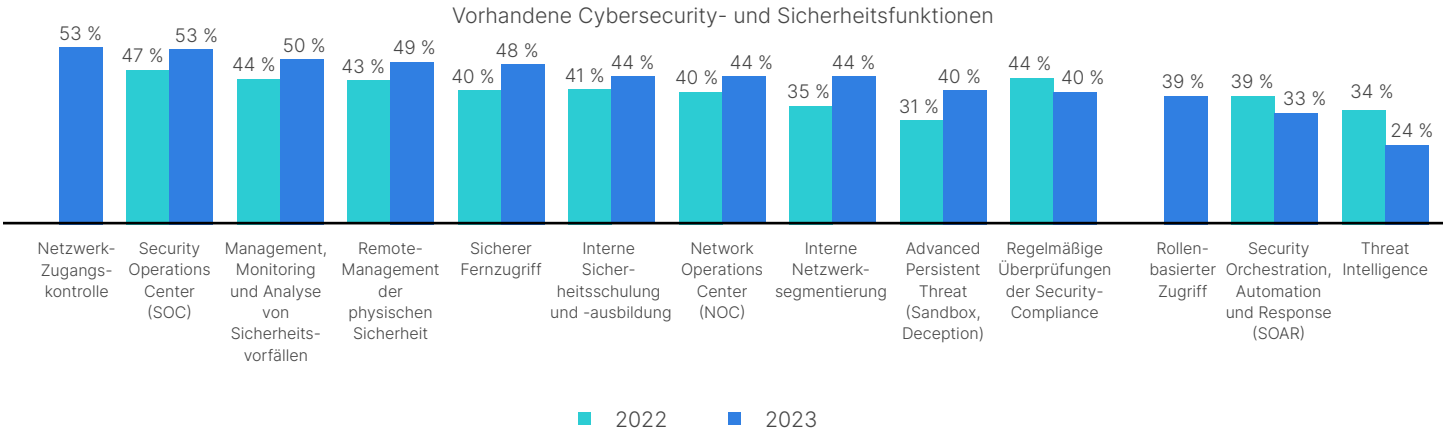
Ausgereiftheit der Cybersecurity			
	Stufe 0–2	Stufe 3	Stufe 4
Weiß nicht	1 %	0 %	0 %
Mehr als 10	1 %	2 %	0 %
6 bis 9	11 %	11 %	6 %
3 bis 5	38 %	35 %	40 %
1 bis 2	36 %[B]	21 %	25 %
0	14 %	31 %[A]	29 %[A]

Folgen von Sicherheitsvorfällen

Von den befragten Unternehmen, die dieses Jahr bereits einen Cyberangriff erlebt hatten, gab fast ein Drittel **(32 %)** an, dass sowohl IT- als auch OT-Systeme betroffen waren – im letzten Jahr waren es nur 21 %. Um Angriffe abzuwehren, erweitern OT-Verantwortliche zunehmend die Cybersecurity-Lösungen in industriellen Netzwerken.

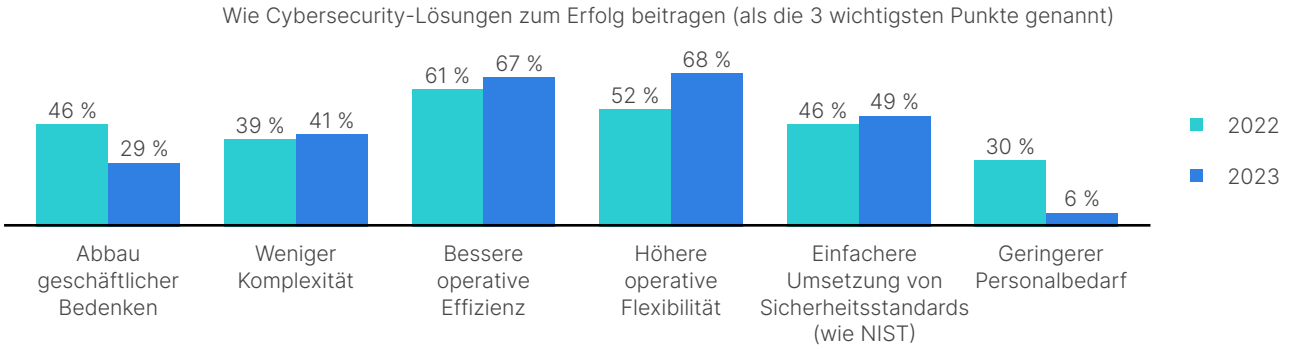


Bei den Bedrohungen haben Advanced Persistent Threats am stärksten zugenommen, bei den Schutzmaßnahmen die interne Netzwerksegmentierung sowie Sicherheitsverbesserungen beim Fernzugriff. Threat-Intelligence-Lösungen werden dagegen weniger genutzt.



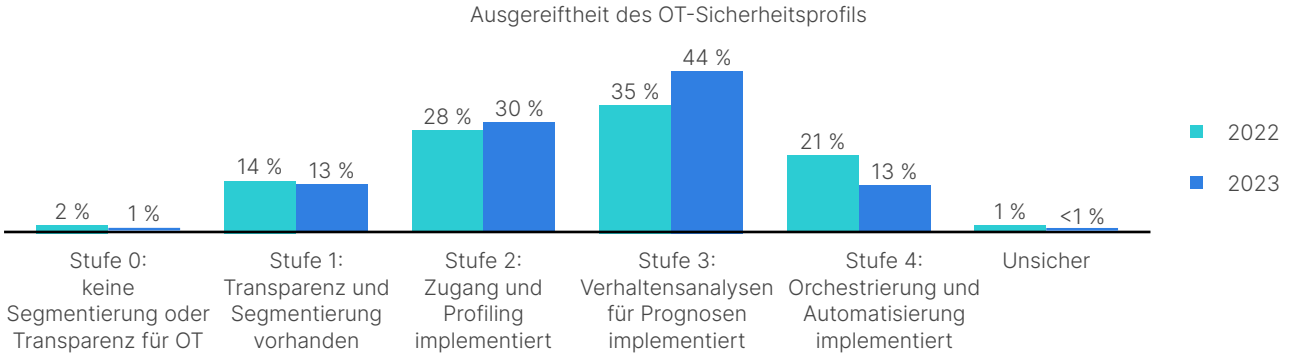
Erfolgsfaktor Cybersecurity

Die Ergebnisse zeigen einerseits, dass Cybersecurity-Lösungen viel zum Erfolg von OT-Verantwortlichen beitragen **(76 %)** – besonders bei der Verbesserung der Wirksamkeit **(67 %)** und Flexibilität **(68 %)**. Andererseits wird ein einheitlicher Schutz konvergierter IT-OT-Umgebungen durch die Fülle an Lösungen immer schwieriger.



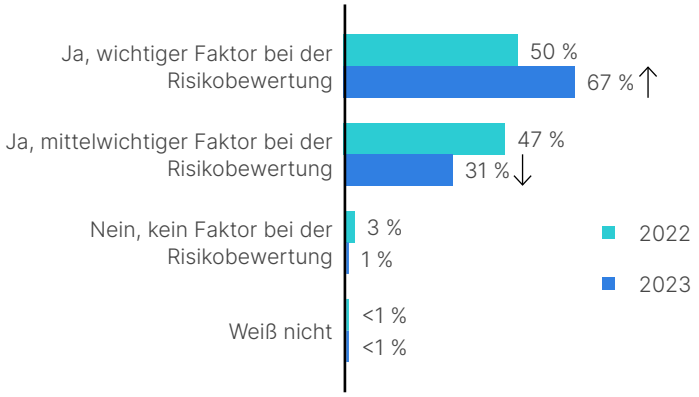
Cybersicherheitsprofil

Während in diesem Jahr verglichen mit 2022 weniger Befragte für ihr OT-Cybersicherheitsprofil die Stufe 4 (sehr ausgereift) angegeben haben (Rückgang um **13 % von 21 %**), sehen sich **44 %** aller Unternehmen bei Stufe 3 – letztes Jahr waren es nur 35 %. Das könnte bedeuten, dass das eigene Sicherheitsprofil realistischer eingeschätzt wird und hier die Bewertungskompetenz gestiegen ist.



Fast jedes Unternehmen (98 %) berücksichtigt mittlerweile bei allgemeinen Risikobewertungen für die Geschäftsleitung und den Vorstand auch das OT-Cybersicherheitsprofil.

Einbeziehung des OT-Sicherheitsprofils bei umfassender Risikobewertung

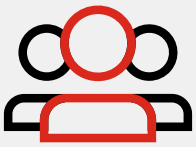


Zusammenfassung

Der jährliche Fortinet-Bericht zum Stand der Betriebstechnologie (OT) und Cybersecurity erscheint 2023 zum fünften Mal. Zugrunde gelegt werden Daten aus der umfassenden weltweiten Befragung von 570 OT-Verantwortlichen, die in unserem Auftrag von einem renommierten Marktforschungsinstitut durchgeführt wurde.

Der Schutz von OT-Systemen ist heute wichtiger denn je, da immer mehr Unternehmen ihre OT-Umgebungen mit dem Internet verbinden. Obwohl die Konvergenz von IT und OT viele Vorteile bringt, wird sie durch hochkomplexe, zerstörerische Cyberbedrohungen erschwert – wodurch Unternehmen nicht vom vollen Potenzial dieser Zusammenlegung profitieren. Dazu kommt, dass Angriffe zunehmend auf OT-Umgebungen abzielen. Aus all diesen Gründen wird die OT-Cybersecurity im aktuellen Risikoportfolio von Unternehmen wichtiger denn je, was auch die Daten unserer Studie belegen.

Aus der Analyse der Ergebnisse von 2023 ergeben sich vier wichtige allgemeine Trends:



Ein Ergebnis des Berichts von 2023: 95 % der Unternehmen haben dem CISO die Verantwortung für die OT-Cybersecurity übertragen.

- Die Zahl der Sicherheitsvorfälle ist wegen weniger Insider-Verstößen zurückgegangen. Trotzdem hat das Cyberrisiko nicht abgenommen. Ransomware und Phishing stellen weiterhin eine große Bedrohung dar, weil Angreifer immer gezielter vorgehen.
- Fast alle Unternehmen haben die Verantwortung für die OT-Cybersecurity einem Chief Information Security Officer (CISO) übertragen statt einem Operations-Manager oder -Team.
- Unternehmen und OT-Experten verlassen sich bei der Bedrohungsabwehr auf unterschiedlichste Cybersecurity-Lösungen. Einiges deutet jedoch darauf hin, dass isolierte Einzelprodukte und die steigende Fülle der eingesetzten Lösungen die Anwendung und Durchsetzung von Richtlinien in konvergierten IT-OT-Umgebungen zunehmend erschweren.
- Mit 13 % vergeben weniger Befragte als im Vorjahr (21 %) für die eigene Cybersecurity die Stufe 4, während zugleich mehr Unternehmen (44 %) ihr Sicherheitsprofil der Stufe 3 zuordnen (2022 waren es noch 35 %). Diese Entwicklung deutet darauf hin, dass OT-Verantwortliche die internen OT-Cybersecurity-Funktionen mittlerweile realistischer einschätzen.

Nach fünf Jahren Befragung von OT-Verantwortlichen ist die ermutigendste Nachricht, dass die Cybersecurity endlich ein zentrales Thema ist und die volle (und regelmäßige) Aufmerksamkeit der Chefetage genießt. Allerdings haben die meisten Unternehmen hier noch eine Menge Arbeit vor sich. Die Cybersecurity sollte zudem als ständige Aufgabe begriffen werden, bei es nie ein „entspanntes Zurücklehnen“ geben wird.

Zur Unterstützung bei der Verbesserung Ihres OT-Sicherheitsprofils enthält dieser Bericht erstmals auch eine Liste grundlegender Best Practices, die Unternehmen mit einer sehr guten Sicherheit beim Schutz von OT-Systemen befolgen.

Einleitung

Heutzutage wird wohl kaum jemand bezweifeln, wie wichtig der Schutz von OT-Systemen ist. Betriebstechnologie steuert die kritischen Infrastrukturen, auf die wir alle angewiesen sind – von Stromnetzen, Wasser- und Abwassersystemen, Verkehrsnetzen und der Herstellung unverzichtbarer Güter bis zu globalen Lieferketten. Darüber hinaus ist Betriebstechnologie in vielen Industrieunternehmen ein Schlüsselelement, um schneller von der Digitalisierung zu profitieren.

Heutige Marktbedingungen sowie Methoden und Technologien der Industrie 4.0 haben ein „Zeitalter der Konnektivität, fortschrittlichen Analytik, Automatisierung und intelligenten Fertigungstechnologie“[1] geschaffen. Nur Unternehmen, die diese Anforderungen erfüllen können, werden ihre Wettbewerbsfähigkeit dauerhaft erhalten. Und das gilt für jede Branche.

Cyberbedrohungen für Betriebstechnologie

Konvergierte IT- und OT-Netzwerke ziehen zunehmend die Aufmerksamkeit von Cyberkriminellen und aggressiven Nationalstaaten auf sich: Wie die aktuellen Global Threat Landscape Reports der FortiGuard Labs zeigen, werden immer mehr Malware und bösartige Aktivitäten in OT-Systemen entdeckt.[2]

Mehrere aufsehenerregende Cyberangriffe verdeutlichen diese Herausforderung und sollten ein Weckruf für alle sein, die für den Schutz von OT-Systemen zuständig sind. Ein Paradebeispiel sind die anhaltenden russischen Angriffe auf die kritische Infrastruktur der Ukraine,[3] die vor über einem Jahr in ein Kriegsgeschehen eskalierten.[4] Allerdings beschränken sich solche Angriffe nicht nur auf offene Aggressionen zwischen Nationalstaaten: Weltweit sind Betriebstechnologie-Systeme nach wie vor das Ziel von Cyberkriminellen. Besonders die Fertigungsbranche hat anhaltend mit vielen gezielten Ransomware-Angriffe auf OT-Systeme zu kämpfen.[5]

Leider ist der Anteil der Unternehmen, die einen Ransomware-Angriff erlebt haben (32 %), gegenüber dem Vorjahr (ebenfalls 32 %) gleich geblieben. Fortschritte bei der Ransomware-Bekämpfung sind also dringend nötig. Und angesichts der Entwicklung sowie zunehmenden Ausgefeiltheit von Ransomware-Angriffen überrascht es kaum, dass 84 % der befragten Unternehmen bei Fortinets weltweiter Ransomware-Studie 2023 wegen dieser Gefahr weiterhin sehr oder äußerst besorgt sind.[6]

Obwohl die Zahl der absichtlichen und unabsichtlichen Insider-Verstöße in diesem Jahr deutlich zurückgegangen ist, haben den Umfrageteilnehmern zufolge Malware- und Phishing-Vorfälle deutlich zugenommen – und zwar um 12 % bzw. 9 %. Diese Ergebnisse bestätigt auch der aktuelle Global Threat Report der FortiGuard Labs, demnach „Malware weiterhin die Schlagzeilen beherrscht und Unternehmen ständig auf Trab hält“.[7]

Kein Schutz mehr durch das Air Gap

Seit der fast durchgängigen Integration von IT- und OT-Infrastrukturen gibt es kein Air Gap mehr, das OT-Systeme früher nahezu unverwundbar gegenüber Cyberangriffen machte. Folglich sind die Angriffsflächen für Industrieunternehmen stark gewachsen. Angesichts des vermehrten Einsatzes von IIoT-Geräten (Industrial Internet of Things), der Gefahr durch bekannte IT-Bedrohungen für anfällige OT-Umgebungen und der Lukrativität von Angriffen auf erfolgskritische Produktionsumgebungen – bei denen Unternehmen schnell bereitwillig Lösegeld zahlen –, wird deutlich, warum der Schutz von Betriebstechnologie heutzutage ein Muss ist.

Schwerpunkt auf die Cybersecurity von Betriebstechnologie (OT)

Im letztjährigen Bericht zum Stand der Betriebstechnologie (OT) und der Cybersecurity[8] erwähnten wir die positive Entwicklung, dass Unternehmen die OT-Cybersecurity zunehmend als zentrales Thema begreifen und stärker darin investieren. Wie die diesjährige Umfrage zeigt, haben viele Firmen jedoch beim angemessenen Schutz ihrer OT-Systeme noch einen weiten Weg vor sich.

Hoffentlich können wir in unserem nächstjährigen Bericht hier große Fortschritte melden. Aber sehen wir uns zunächst an, welcher aktuelle Stand der OT-Cybersecurity sich aus den aktuellen Umfrageergebnissen ableiten lässt.

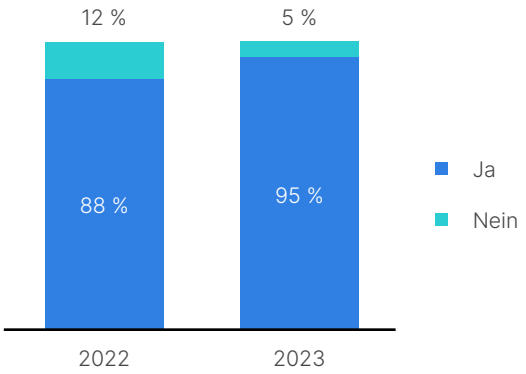
Wesentliche Erkenntnisse

1. Erkenntnis: Die Zuständigkeit für die OT-Cybersecurity verlagert sich vom Betriebstechnologie-Team zu Experten für die Cybersicherheit.

OT-Mitarbeiter sind in fast allen wichtigen Branchen zu finden, wie Fertigung, Transport, Logistik, Gesundheitswesen, Pharmazeutik, Öl, Gas, Energie, Versorgung, Chemie, Wasser, Abwasser und anderen Sektoren. Traditionell sind diese OT-Fachleute auch maßgeblich an Kaufentscheidungen für die Cybersicherheit von OT-Umgebungen beteiligt.

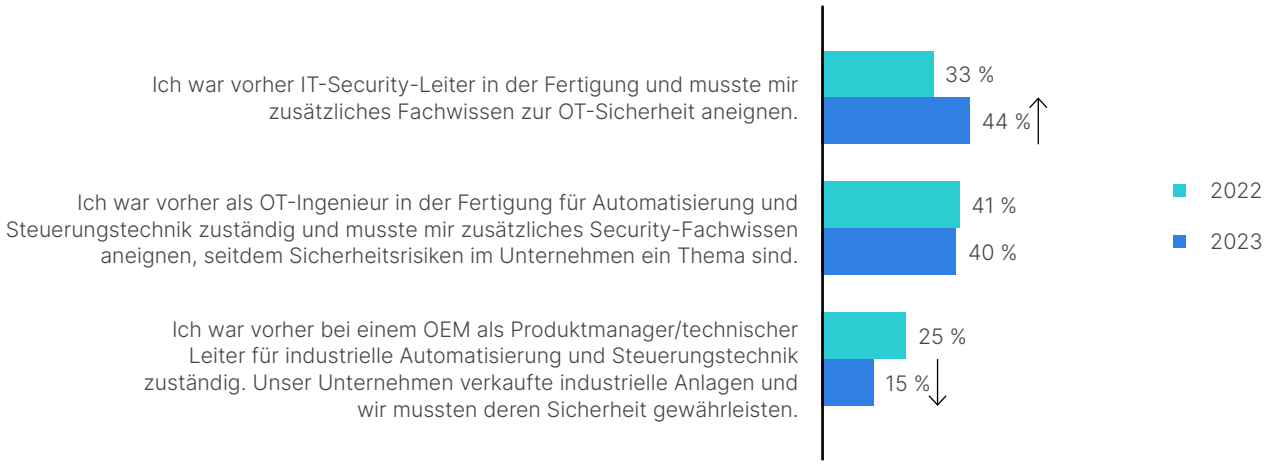
Offensichtlich hat die anhaltende Anfälligkeit von OT-Netzwerken für Cyberangriffe dazu geführt hat, dass der CISO vermehrt für die Cybersicherheit von Betriebstechnologie zuständig ist. Wie die Umfrageergebnisse zeigen, stammen die neuen OT-Sicherheitsexperten eher aus dem IT-Team als aus dem Produktmanagement. Außerdem werden die Chefetage und die seit jeher für die Sicherheit Verantwortlichen – insbesondere der CISO/CSO – jetzt stärker bei Entscheidungsprozessen und Investitionen in die Cybersecurity einbezogen.

Frage: Plant Ihr Unternehmen, die OT-Cybersecurity in den nächsten 12 Monaten dem CISO zu unterstellen?



Cybersecurity wird in den nächsten 12 Monaten dem CISO unterstellt

Frage: Welcher berufliche Hintergrund hat Sie zur OT-Sicherheit gebracht?

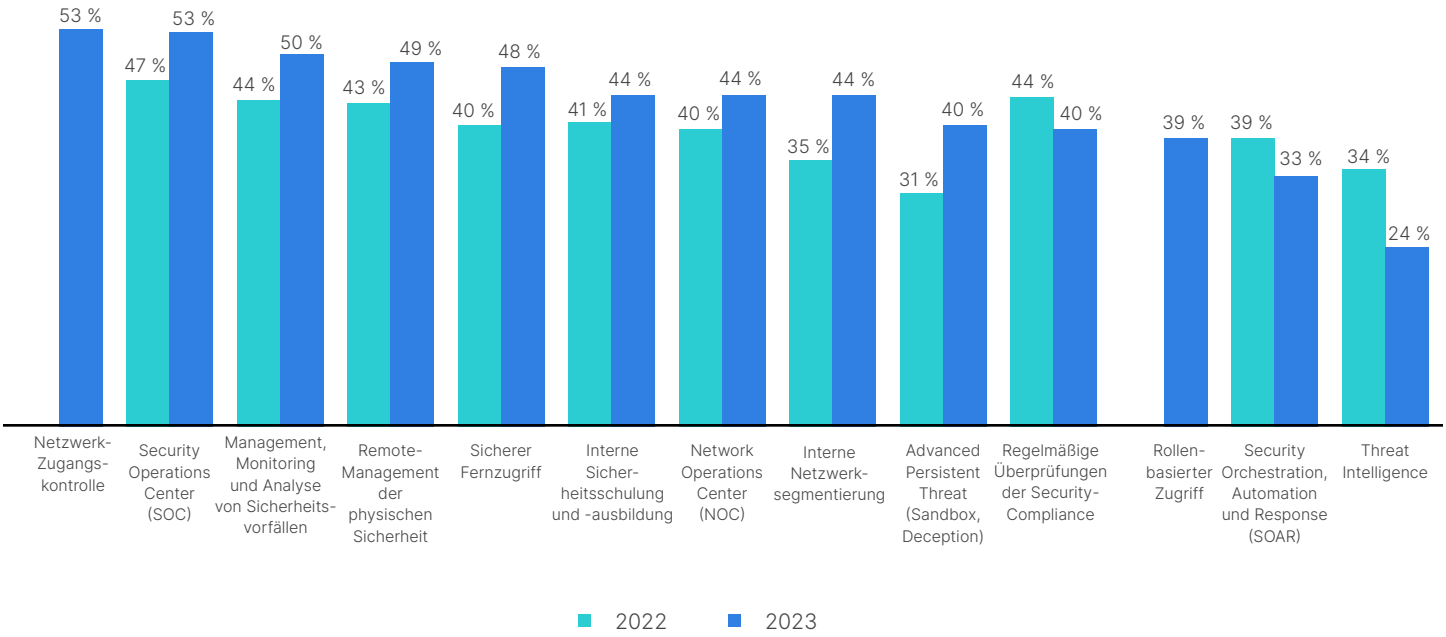


Beruflicher Hintergrund von OT-Security-Verantwortlichen

2. Erkenntnis: OT-Verantwortliche verlassen sich auf viele Lösungen.

Die in diesem Jahr befragten OT-Experten achten bei einer Cybersecurity-Lösung vor allem darauf, dass sie bekannte Schwachstellen erkennen kann. Eine besondere Herausforderung für OT-Teams ist die Gefahr von Ausfallzeiten, die bei Betriebstechnologie meistens ernstere Konsequenzen als in IT-Umgebungen haben. An erster Stelle steht daher die Verfügbarkeit kritischer Systeme. Erst danach kommt die Wahrung der Vertraulichkeit und Integrität von Daten. Folglich ist die Reaktionszeit auf Angriffe besonders wichtig, was sich an der häufigeren Implementierung von OT-Netzwerk- und Cybersecurity-Lösungen zeigt.

Aber wie bei IT-Netzwerken reicht es nicht aus, lediglich alle Angriffe auf OT-Netzwerke zu verhindern. Hinzu kommt, dass sehr viele Lösungen von verschiedensten Herstellern eingesetzt werden. Das erschwert nicht nur die Erkennung von Bedrohungen, sondern verhindert auch eine koordinierte Abwehrreaktion.



Vorhandene Cybersecurity- und Sicherheitsfunktionen

3. Erkenntnis: Die Anzahl der Sicherheitsvorfälle ist weiterhin besorgniserregend.

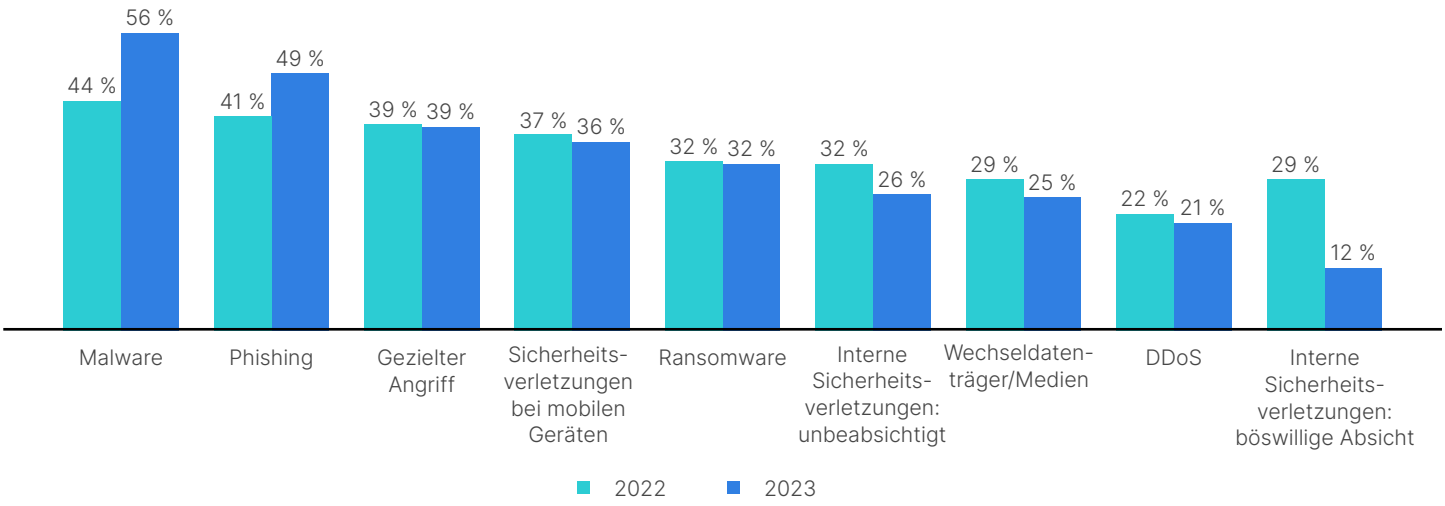
Trotz abnehmender Sicherheitsvorfälle berichten weiterhin 75 % der befragten Unternehmen von mindestens einem illegalen Netzwerkzugriff in den letzten 12 Monaten. Der Grund für diesen Gesamtrückgang sind weniger Insider-Verstöße, nicht weniger Angriffe von Cyberkriminellen.

Malware- und Phishing-Vorfälle sind nach wie vor die häufigsten Bedrohungen und haben gegenüber dem Vorjahr zugenommen. Ransomware bleibt die größte Bedrohung – und die Zahl der Angriffe steigt weiter. Die Folgen von Angriffen waren unterschiedlichster Natur, betrafen zunehmend IT- und OT-Systeme, konnten aber in der Regel innerhalb von Stunden (und immer öfter auch in Minuten) behoben werden.

Teilweise dürften die rückläufigen Sicherheitsvorfälle auf eine geänderte Taktik der Cyberkriminellen zurückgehen. Die Effektivität der Angriffe ist jedoch ungebrochen, wie die Zunahme von Malware und Phishing zeigt. Angesichts des hohen Werts von OT-Systemen sind noch mehr gezieltere Angriffe nur eine Frage der Zeit.

Es ist wichtig darauf hinzuweisen, dass ein überhöhtes Vertrauen in die Stärke der eigenen Sicherheitsmaßnahmen Unternehmen genauso schadet wie die Implementierung der falschen Technologien. Letzteres ist ein weiteres Problem, wie unser aktueller Ransomware-Bericht[9] zeigt: Für die meisten Unternehmen besitzt der Schutz vor Ransomware hohe Priorität – und gleichzeitig werden Lösungen als unverzichtbar für die Cybersecurity-Strategie erachtet, die kaum vor Ransomware schützen.

Frage: Welche Arten von Sicherheitsvorfällen gab es? (Alles Zutreffende ankreuzen)



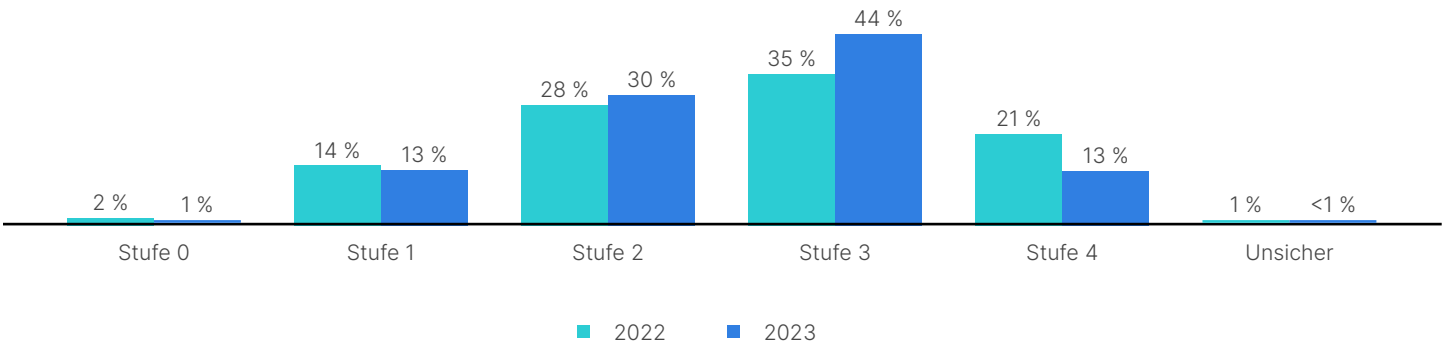
Stattgefundene Sicherheitsvorfälle

4. Erkenntnis: Die durchschnittliche Sicherheitsstufe bei der Cybersecurity verbessert sich.

Eine korrekte Bewertung vorhandener Cybersecurity-Funktionen und des Reifegrads des eigenen Sicherheitsprofils ist ein wichtiger erster Schritt, um die Cyberabwehr zu verbessern und OT-Umgebungen angemessen zu schützen. Weltweit stufen in diesem Jahr weniger Unternehmen (13 %) ihr OT-Sicherheitsprofil als sehr ausgereift ein – 2022 waren es noch 21 %. Gleichzeitig sehen 44 % der Unternehmen ihr OT-Cybersicherheitsprofil jetzt auf Stufe 3 (gegenüber 35 % im Vorjahr). Diese Daten deuten auf eine realistischere Selbsteinschätzung der eigenen OT-Cybersecurity bei den Befragten hin.

Ausgereiftheit – die Sicherheitsstufen	
Stufe 0	Keine Segmentierung oder Transparenz für OT
Stufe 1	Transparenz und Segmentierung vorhanden
Stufe 2	Zugangskontrolle und Profiling eingerichtet
Stufe 3	Verhaltensanalysen für Prognosen implementiert
Stufe 4	Orchestrierung und Automatisierung

Frage: Wie würden Sie die Ausgereiftheit Ihres OT-Sicherheitsprofils beschreiben?

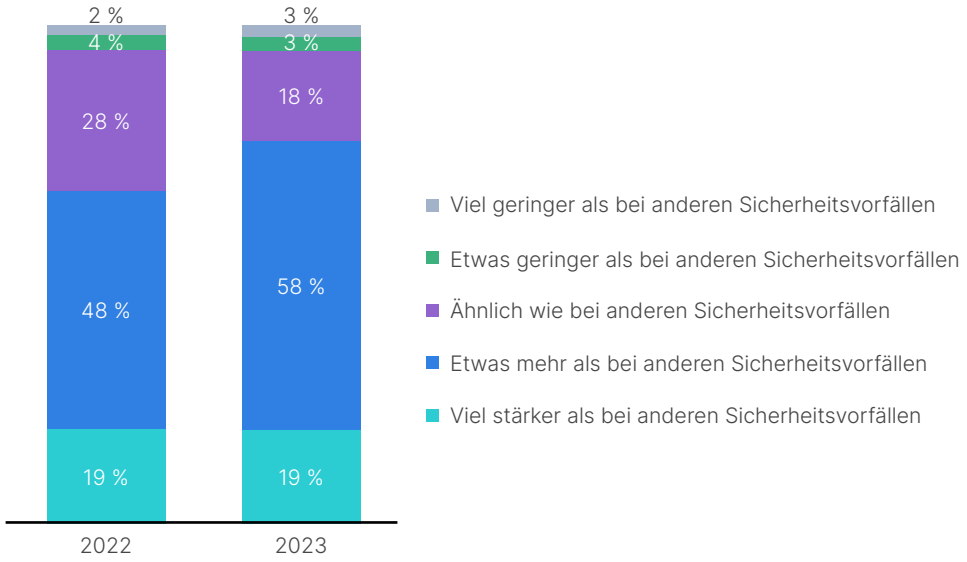


Ausgereiftheit des OT-Sicherheitsprofils

Interessante Ergebnisse im Detail

Frage: Wie besorgt sind Sie wegen Ransomware-Angriffen auf Ihre OT-Umgebung verglichen mit anderen Sicherheitsvorfällen?

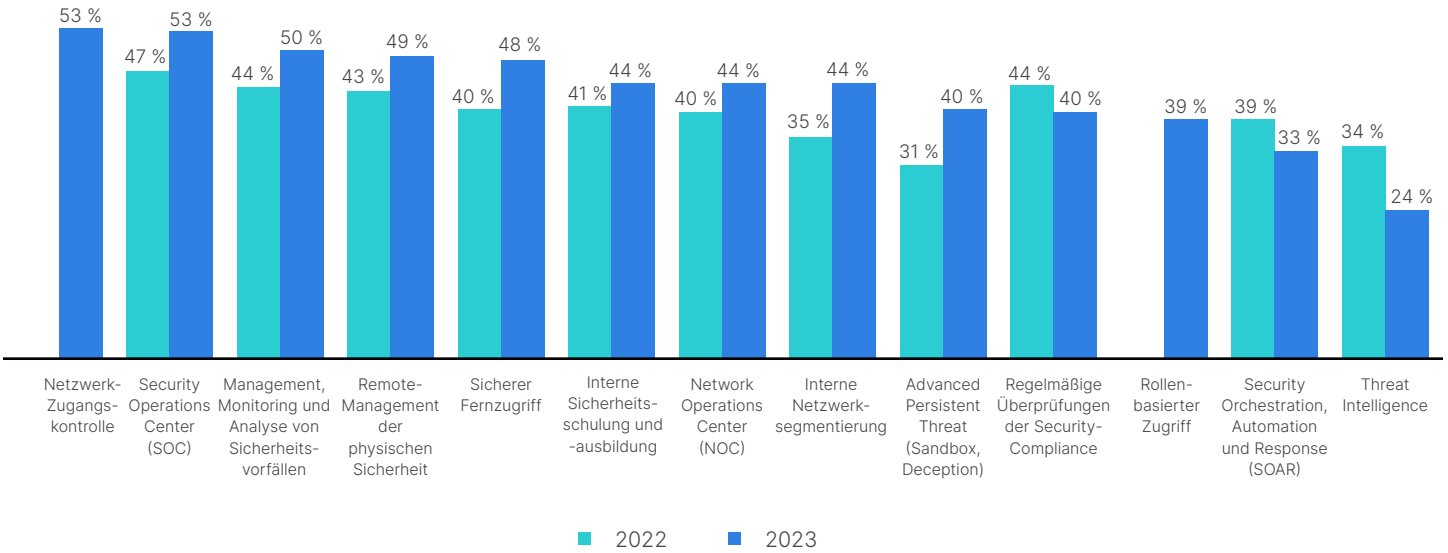
Ransomware-Vorfälle im Unternehmens- oder IT-Netzwerk können sich direkt oder indirekt auf die Produktion auswirken. Unternehmen machen sich deswegen zunehmend mehr Sorgen als über andere Sicherheitsvorfälle (obwohl Phishing und Malware häufiger vorkommen). Daher bleibt Ransomware wegen ihrer Auswirkungen auf die Fertigung und der finanziellen Folgen eine der am stärksten wahrgenommenen Cybergefahren.



Besorgnis über die Auswirkungen von Ransomware

Frage: Welche Cybersecurity- und Sicherheitsfunktionen setzen Sie derzeit ein?

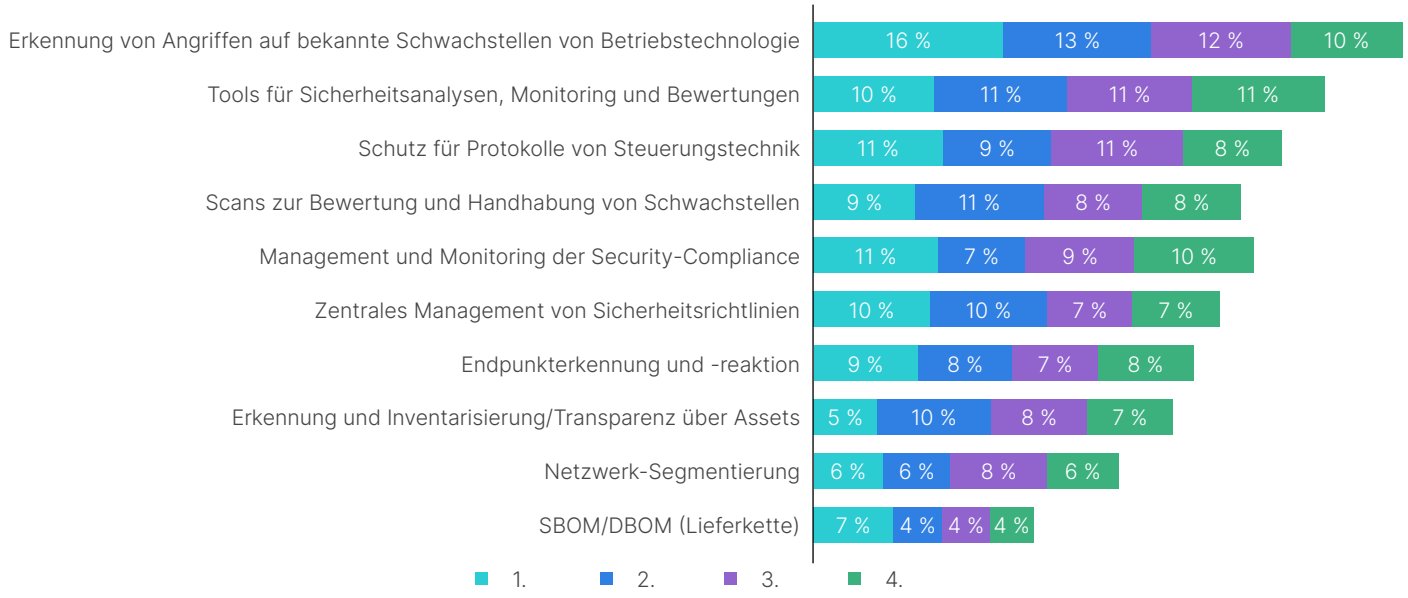
Im Kampf gegen Angriffe und Bedrohungen verstärken OT-Verantwortliche nun die zahlreichen vorhandenen Cybersecurity- und Verteidigungsfunktionen. Wir vermuten, dass der Rückgang der Security Audits mit diesen zusätzlichen Sicherheitsfunktionen sowie fortschrittlicheren Lösungen wie SOAR und Threat Intelligence zusammenhängt. Sobald die neuen Sicherheitsfunktionen implementiert sind, dürfte die Anzahl der Audits wieder das vorherige Niveau erreichen.



Vorhandene Cybersecurity- und Sicherheitsfunktionen

Frage: Welche Funktionen sind bei OT-Cybersecurity-Lösungen am wichtigsten? (Bitte bis zu 4 Funktionen in der Rangfolge ihrer Wichtigkeit angeben.)

Die Erkennung von Angriffen auf bekannte Schwachstellen gilt mittlerweile als wichtigste Funktion von Cybersecurity-Lösungen und hat im letzten Jahr noch mehr an Bedeutung gewonnen. Ein weiteres Indiz für die zunehmende Ausgereiftheit der OT-Security ist die geringere Priorität, die der Erkennung, Inventarisierung und Segmentierung von Ressourcen zugemessen wird. Was wir im OT-Bereich beobachten, bestätigt auch der Implementierungsleitfaden für industrielle Steuerungssysteme (ICS) von CIS Controls[10]: Die meisten Unternehmen verfügen über eine rudimentäre Security und führen derzeit fortschrittlichere, grundlegende und unternehmensweite Lösungen ein.

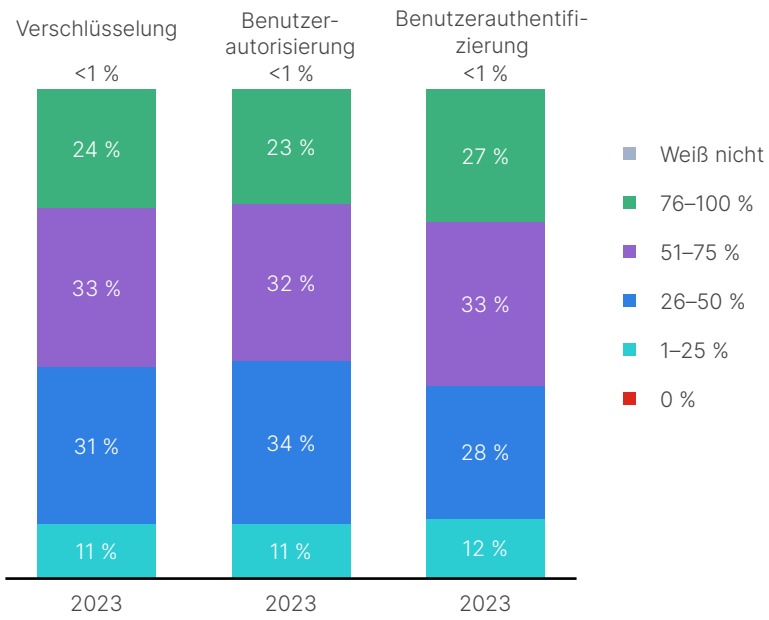


Wichtigste Funktionen bei Cybersecurity-Lösungen (Ranking)

Frage: Wie viel Prozent Ihrer SPS oder RTU nutzen jede der folgenden Sicherheitsfunktionen?

Verschlüsselung, Benutzerautorisierung und Benutzerauthentifizierung werden tendenziell für über 50 % der SPS oder RTU verwendet.

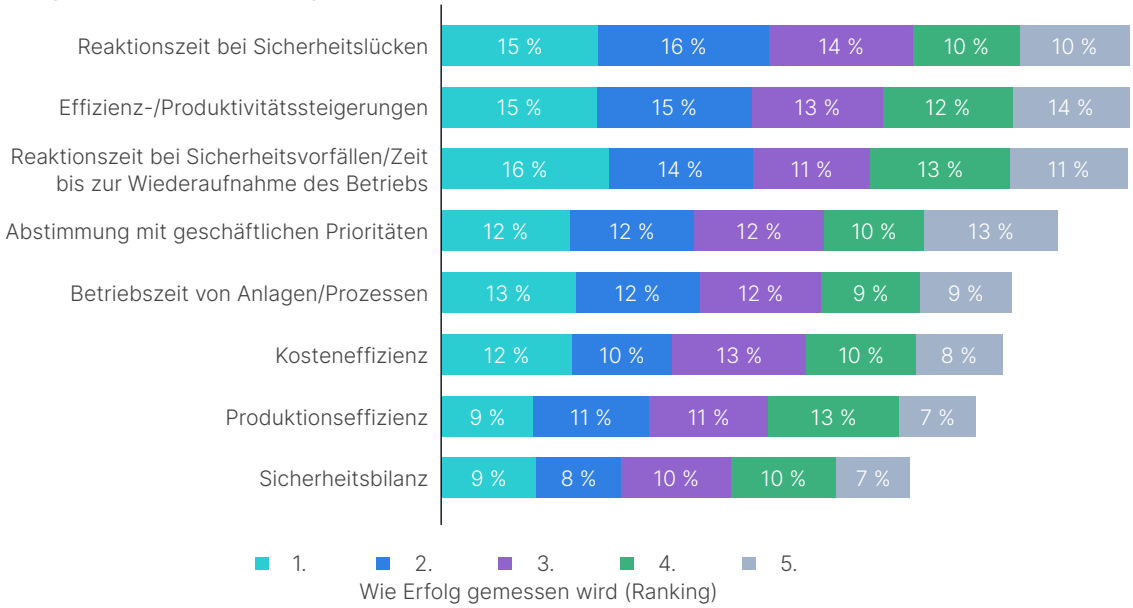
Anteil der SPS oder RTU, die Folgendes verwenden:



Allgemeine Auswirkungen

Frage: Wie wird Ihr Erfolg gemessen? (Bitte bis zu 5 Kriterien in der Rangfolge ihrer Wichtigkeit angeben.)

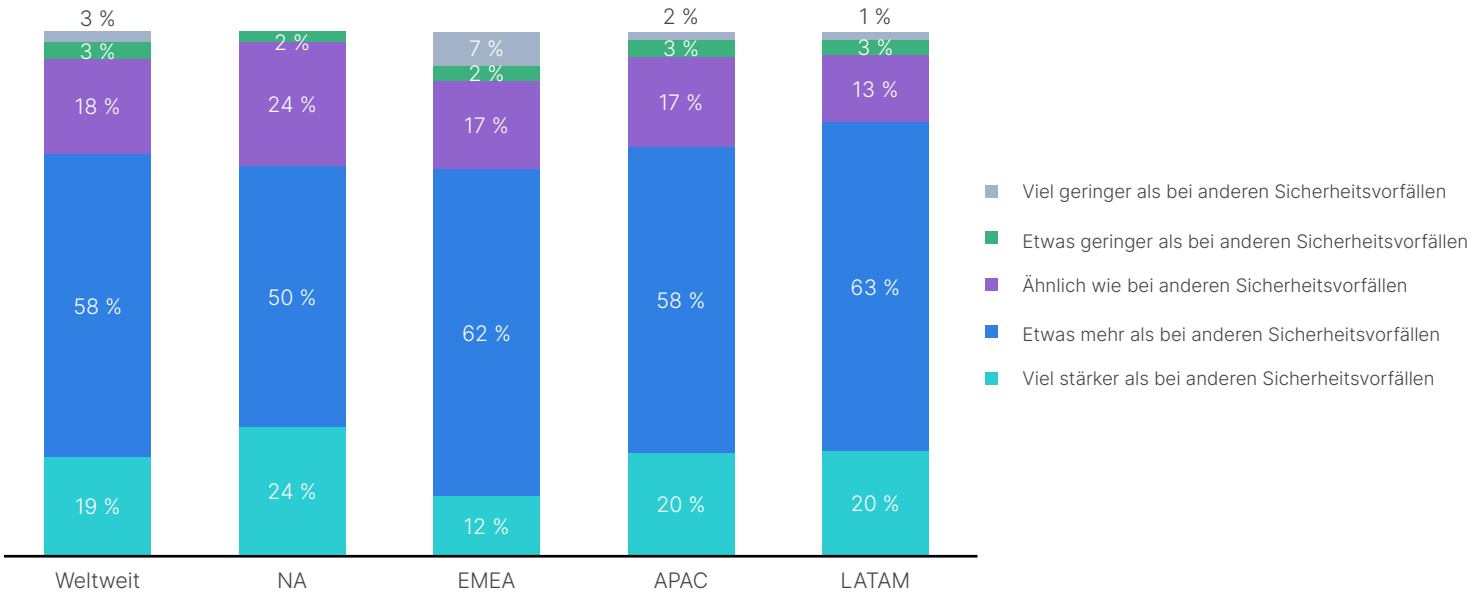
Interessanterweise gibt es bei Betriebstechnologie keine einheitliche Erfolgsdefinition. Das deutet auf die generelle Unausgereiftheit der OT-Security hin. Andererseits gelten für OT-Umgebungen andere Prioritäten: Reaktionszeiten und Produktivitätssteigerungen sind hier am wichtigsten.



Wie Erfolg gemessen wird (Ranking)

Frage: Wie besorgt sind Sie wegen Ransomware-Angriffen auf Ihre OT-Umgebung verglichen mit anderen Sicherheitsvorfällen?

Obwohl Ransomware-Angriffe nicht zu den häufigsten Sicherheitsvorfällen zählen, bereiten sie weltweit den meisten Unternehmen die größten Sorgen (mehr als alle anderen Bedrohungen). Das liegt wahrscheinlich an ihrer Bekanntheit und der hohen Kosten für die Wiederherstellung betroffener Systeme nach einem Angriff.



Besorgnis über die Auswirkungen von Ransomware

Best Practices

75 % der teilnehmenden Unternehmen berichteten von mindestens einen Sicherheitsvorfall in den letzten 12 Monaten. Ob Sie es glauben oder nicht: Das ist eine Verbesserung gegenüber 2022, als über 90 % mindestens einen Vorfall angaben. Außerdem meldeten dieses Jahr nur 11 % der Befragten sechs oder mehr Sicherheitsvorfälle – im Vorjahr waren es noch 27 %.

Zwar tragen Cybersecurity-Lösungen weiterhin zum Erfolg der meisten (76 %) OT-Verantwortlichen bei – insbesondere durch die Verbesserung der Wirksamkeit (67 %) und Flexibilität (68 %). Doch die Ergebnisse zeigen auch, dass die Integration, Anwendung und Durchsetzung einheitlicher Richtlinien in zunehmend konvergierten IT-OT-Umgebungen wegen der Fülle der Sicherheitslösungen schwierig bleibt. Dieses Problem verschärft sich durch veraltete Systeme: Die Mehrheit (74 %) der Befragten gibt als Durchschnittsalter ihrer ICS-Systeme 6 bis 10 Jahre an. Zweifelslos haben Unternehmen bei der allgemeinen OT-Cybersecurity einige Fortschritte erzielt, aber das Engagement darf jetzt nicht abreißen.

Im Folgenden finden Sie einige Best Practices, auf die unserer Ansicht nach die kleine, aber deutliche Verbesserung der diesjährigen Umfrageergebnisse zurückzuführen ist.

Plattform-Strategie für Anbieter und OT-Cybersecurity

Konsolidierungen verringern die Komplexität und führen zu schnelleren Ergebnissen. Der erste Schritt besteht im sukzessiven Aufbau einer Plattform. Ideal ist die Zusammenarbeit mit Anbietern, die ihre Produkte für eine bessere Integration und Automatisierung weiterentwickeln. Entscheidend ist, dass der Anbieter die Festlegung und Durchsetzung einheitlicher Richtlinien in zusammenwachsenden IT- und OT-Umgebungen unterstützt. Außerdem sollte der ideale Anbieter ein breites Portfolio an Lösungen haben, mit denen Sie sowohl eine grundlegende Inventarisierung und Segmentierung als auch fortschrittlichere Sicherheitsfunktionen wie ein OT-SOC oder die Unterstützung eines gemeinsamen IT-OT-SOC erhalten.

Einsatz einer Netzwerkzugangskontrolle (NAC)

Zur Lösung von Herausforderungen beim Schutz von industriellen Steuerungssystemen (ICS), Supervisory Control and Data Acquisition (SCADA), dem Internet der Dinge (IoT), Bring Your Own Device (BYOD) sowie anderen Endpunkten ist eine fortschrittliche Netzwerkzugangskontrolle (Network Access Control, NAC) als Teil einer umfassenden Sicherheitsarchitektur unverzichtbar. Eine wirksame NAC-Lösung hilft auch dabei, die vollständige Kontrolle über das Unternehmensnetzwerk zu behalten: Sie vereinfacht das Management neuer Geräte, die sich mit anderen Teilen der Unternehmensinfrastruktur verbinden bzw. kommunizieren möchten.

Einführung eines Zero-Trust-Ansatzes

Die Implementierung einer grundlegenden Asset-Inventarisierung und -Segmentierung darf auf keinen Fall fehlen. Ein Zero-Trust-Access (ZTA) bietet eine kontinuierliche Überprüfung aller Benutzer, Anwendungen und Geräte, die auf wichtige Ressourcen zugreifen wollen – unabhängig davon, wo sie sich befinden.

Aufklärung und Schulungen zur Cybersecurity

Schulungen zum Thema Cybersecurity sind eigentlich immer ein Muss, weil der Kampf gegen Cyberkriminelle die gesammelte Kompetenz aller Mitarbeiter erfordert. Jeder im Unternehmen muss über Sicherheitsmaßnahmen und Angriffsformen gut Bescheid wissen. Nur wenn Mitarbeiter sich selbst und die Unternehmensdaten wirksam schützen können – und bei Sicherheitsfragen zusammenarbeiten – steht die Security auf soliden Füßen. Eine gute Idee sind auch nichttechnische Schulungen z. B. für alle Geräte (Computer, Tablets, Smartphones), Homeoffice-Mitarbeiter und deren Angehörige.

Top-Tipps für mehr Sicherheit

1. Setzen Sie die grundlegende Inventarisierung und Segmentierung fort. Führen Sie als Nächstes fortschrittlichere Lösungen für die Mikrosegmentierung und ein virtuelles Patching ein. Damit schützen Sie Geräte vor bekannten Schwachstellen und gewinnen genug Zeit bis zum geplanten Wartungstermin, um dann das richtige Patching anzuwenden.

2. Arbeiten Sie mit IT-, OT- und Produktionsteams zusammen, um Cyber- und Produktionsrisiken – insbesondere Ransomware-Vorfälle – richtig einzuschätzen und den CISO zu informieren. So schaffen Sie ein solides Sicherheitsbewusstsein, setzen die richtigen Prioritäten und können Budget- und Personalzuweisungen sicherstellen.
3. Entwickeln Sie eine Plattform-Strategie für Anbieter und die OT-Cybersecurity. Oft werden viele neue Sicherheitslösungen eingeführt, während gleichzeitig immer mehr qualifizierte Fachkräfte fehlen. Wenn Sie ein stärkeres Sicherheitsprofil erreicht haben, suchen Sie sich am besten einen Anbieter mit einem breitgefächerten Portfolio, das von grundlegenden Lösungen für die Inventarisierung und Segmentierung bis hin zu fortschrittlicheren Lösungen wie einem OT-SOC oder der Unterstützung eines gemeinsamen IT-OT-SOC reicht.

Methodik dieser Studie

Der Großteil der Befragten stammt aus einem Werks- oder Fertigungsbetrieb (mit Stellenbezeichnungen wie „Plant Operations“ oder „Manufacturing Operations“), wobei fast ein Drittel der Studienteilnehmer zum leitenden Management gehören („Vice President“ oder „Director of Plant Operations“). 91 % der Befragten sind in ihrem Unternehmen regelmäßig in Kaufentscheidungen im Bereich Cybersecurity involviert – unabhängig von ihrer Stellenbezeichnung – und haben zugleich oft das letzte Wort bei der Anschaffung von Betriebstechnologie.

Alle Teilnehmer an der diesjährigen Umfrage arbeiteten in einer der folgenden Branchen:

- Fertigung
- Transportwesen, Logistik
- Gesundheitswesen, Pharma
- Öl, Gas, Raffination
- Energie, Versorger
- Chemie, Petrochemie
- Wasser, Abwasser

Ziele der Studie

Fortinet beauftragte das externe Marktforschungsinstitut InMoment mit der Unterstützung bei der Entwicklung einer OT-Experten-Persona.

Die von InMoment mitgestaltete Umfrage sollte ein besseres Verständnis darüber eröffnen,

- welche Rolle die Persona in Unternehmen übernimmt,
- wie Sicherheitsfunktionen genutzt werden,
- wie Informationen nachverfolgt und in Berichten erfasst werden sowie
- welche Einflüsse und Erfolgsfaktoren es gibt.

Befragungsansatz

Mithilfe einer Panel-Stichprobe wurden 570 vollständige, abgeschlossene Befragungen vom folgenden Teilnehmertyp aus einem Unternehmen in diesen Branchen eingeholt:

- Fertigung
- Transportwesen, Logistik
- Gesundheitswesen, Pharma

- Öl, Gas, Raffination
- Energie, Versorger
- Chemie, Petrochemie
- Wasser, Abwasser
  - mit über 1.000 Beschäftigten, einschließlich ausgewählter Ausnahmen
- Betriebstechnologie (OT) gehört zum Zuständigkeitsbereich der Funktion
- Hat berichtsbezogene Verantwortung für die Fertigung oder den Anlagenbetrieb
- Ist an Cybersecurity-Kaufentscheidungen beteiligt
- Erweiterte globale Reichweite 2022 und 2023:
  - Die Befragten stammten aus verschiedenen Ländern, u. a. aus Deutschland, Frankreich, Großbritannien, Australien, Ägypten, Brasilien, Indien, Japan, Kanada, Mexiko, Neuseeland, Südafrika und den USA.

Fazit

Wie dieser Bericht zum Stand der Betriebstechnologie (OT) und der Cybersecurity 2023 zeigt, genießt die Cybersecurity von OT-Umgebungen in Unternehmen zunehmend Priorität. Dies ist ein wichtiger – und notwendiger – Trend, da 75 % der befragten Unternehmen in den letzten 12 Monaten mindestens einen Cyberangriff erlebten. Die Umfrageergebnisse deuten darauf hin, dass sich die Cybersecurity von Betriebstechnologie verbessert bzw. immer ausgereifter wird und die Vorfälle anscheinend abnehmen. Gleichzeitig werden die mit OT-Sicherheitsvorfällen verbundenen Risiken durch die weltweiten Ereignisse deutlicher. Zudem gehen Unternehmen mittlerweile die Verbesserung ihres OT-Sicherheitsprofils engagierter an und IT-Teams haben bei industriellen Netzwerken mehr Mitspracherechte.

Die Umfrageergebnisse zeigen eine allgemeine Zunahme verschiedener OT-Cybersecurity-Lösungen, einhergehend mit einem wachsenden Reifegrad der Cybersecurity von Betriebstechnologie, besser abgegrenzten Zuständigkeiten sowie der Implementierung von Sicherheitslösungen. All das führt zu Verbesserungen, allerdings haben die meisten Unternehmen beim angemessen Schutz vor der häufigsten Malware wie Ransomware noch einen langen Weg vor sich.

[1] „What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?“. McKinsey and Company, 17. August 2022.

[2] 2022 Global Threat Landscape Report, FortiGuard Labs, 22. Februar 2023. (Deutsche Ausgabe erhältlich. Bitte fragen Sie Ihren Ansprechpartner bei Fortinet.)

[3] „Cyber-Attack Against Ukrainian Critical Infrastructure“. CISA, 20. Juli 2021.

[4] „Ukraine: Russian attacks on critical energy infrastructure amount to war crimes“. Amnesty International, 22. Oktober 2022.

[5] Jonathan Reed: „Pipedream Malware Can Disrupt or Destroy Industrial Systems“. Security Intelligence, 19. April 2023.

[6] The 2023 Global Ransomware Report, Fortinet, 24. April 2023.

[7] 2022 Global Threat Landscape Report, FortiGuard Labs, 22. Februar 2023. (Deutsche Ausgabe erhältlich. Bitte fragen Sie Ihren Ansprechpartner bei Fortinet.)

[8] „2022 State of Operational Technology and Cybersecurity“. Fortinet, 21. Juni 2022. (Deutsche Ausgabe erhältlich. Bitte fragen Sie Ihren Ansprechpartner bei Fortinet.)

[9] The 2023 Global Ransomware Report, Fortinet, 24. April 2023.

[10] „CIS Critical Security Controls ICS Companion Guide“. Center for Internet Security, Version 7.

7. August 2023, 11:23 Uhr

2101968-0-0-DE