Industrial Security 2019: ein Ausblick von TÜV Rheinland

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

Inhaltsverzeichnis

Zusammenfassung

UNZUREICHENDE CYBERSECURITY FÜR OPERATIONAL TECHNOLOGY (OT) HAT AUSWIRKUNGEN AUF DIE AKQUISE NEUER AUFTRÄGE

Die moderne Industrie, ob Fertigung, Telekommunikation, Versorgungswirtschaft, Transport oder Energieerzeugung/-versorgung, durchläuft derzeit einen bedeutenden Wandel, da neue Technologien bessere Möglichkeiten zur Entwicklung, Realisierung und Lieferung von Produkten und Dienstleistungen bieten. Der Einsatz moderner Technologien geht jedoch mit der Gefahr zunehmender Bedrohungen der Cybersecurity im Bereich der Operational Technology einher. Darüber hinaus muss der Betrieb industrieller OT-Systeme den Schutz vertraulicher Produktionsdaten entlang der gesamten Lieferkette gewährleisten. Produktionssysteme müssen ein hohes Maß an Sicherheit und Produktivität aufweisen. Das Fehlen einer geeigneten OT-Cybersecurity-Umgebung kann direkte Auswirkungen auf die Möglichkeit haben, neue Verträge und Aufträge zu gewinnen. Kunden teilen nur ungern geistiges Eigentum, Material und Designs mit Einrichtungen, die anfällig für Cyber-Bedrohungen sind.

REGELUNGEN IM ZUSAMMENHANG MIT CYBERSECURITY MÜSSEN AUF DIE ANFORDERUNGEN VON OT ZUGESCHNITTEN SEIN

Viele OT-Systeme sind im Laufe der Zeit gewachsen. Dadurch ist ein schier grenzenloses Risikoumfeld entstanden, denn Unternehmen haben Schwierigkeiten, die entsprechenden Anlagen und Netzwerke zu schützen und zu überwachen. Ohne Kenntnis aller zu sichernden OT-Komponenten und deren laufende Überwachung ist es äußerst schwierig, eine OT-Umgebung zu sichern. Diese Aufgabe wird durch die Verknüpfung von betrieblichen IT-Systemen mit der OT-Umgebung der Produktion und durch die Anwendung herkömmlicher Informationssicherheitskontrollen auf die oft speziellen Anforderungen von OT-Systemen weiter erschwert. Häufig wird dieses Problem durch die Anwendung ungeeigneter IT-Richtlinien und -Prozeduren noch verschärft. Richtlinien und Verfahren im Zusammenhang mit Cybersecurity müssen auf die besonderen Anforderungen von OT zugeschnitten sein. Dazu müssen in den Produktionsstätten und -anlagen spezifische Maßnahmen umgesetzt werden. Die Anwendung der jeweils gültigen aktuellen IT-Sicherheitsrichtlinien allein ist nicht ausreichend.

WACHSENDE NACHFRAGE NACH BESSERER CYBERSECURITY

Reaktionspläne für OT-Cybersecurity-Vorfälle müssen regelmäßig geübt werden, damit alle Beteiligten ihre Rollen und Verantwortlichkeiten kennen. So werden auch Änderungen von Personal, Prozessen oder Technologien erfasst, die Auswirkungen auf die Ausführung eines Plans haben. Sobald ein Vorfall im Zusammenhang mit OT-Cybersecurity behoben wurde, muss der gewohnte Betrieb so schnell wie möglich wieder aufgenommen werden. Ein Wiederherstellungsplan muss alle Schritte abdecken, die z. B. für den Wiederaufbau von OT-Systemen und -Ressourcen erforderlich sind. Wenn für eine solche Wiederherstellung kein Plan erstellt wird, kann dies erhebliche Auswirkungen auf den Neustart der Systeme haben, was Zeit kosten kann. Die Gefährdung eines industriellen Systems durch einen Cyberangriff kann zu einer Umweltkatastrophe, schweren Verletzungen oder sogar zu Todesfällen führen. Die Cybersecurity von OT-Systemen muss durch eine angemessene, risikobasierte Evaluierung und durch umfassend budgetierte und finanzierte Cybersecurity-Kontrollmaßnahmen gewährleistet werden.

Dieser Ausblick auf 2019 prognostiziert eine wachsende Nachfrage nach einer verbesserten Cybersecurity für OT und empfiehlt, frühzeitig vorbeugende Maßnahmen zu ergreifen.

Ausblick 2019 – die nächsten Schritte

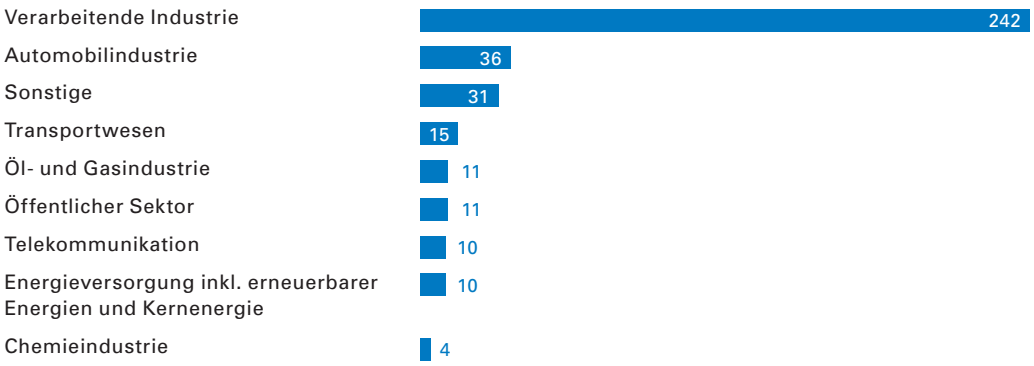
1. Mit der Zunahme gezielter Hacker-Angriffe auf OT ist es von entscheidender Bedeutung, dass Organisationen ihr OT-Cybersecurity-Risiko explizit als einen separaten handlungsbedürftigen Posten in ihrem Budget betrachten.
2. Implementierung von Netzwerküberwachung, Bestandserfassung und -verwaltung für alle OT-Systeme. Kapazitäten müssen entwickelt werden, um effektiv auf kritische Ereignisse oder Vorfälle reagieren zu können.
3. Mit OT-Systemen arbeitendes Personal und Produktionsteams müssen umfassend eingebunden werden, da sie eine bedeutende Rolle bei der Gewährleistung der Cybersecurity spielen.
4. Die Kontrollen, Richtlinien und Verfahren für IT-Cybersecurity sollten aktualisiert werden, um sicherzustellen, dass OT-Systeme vollständig integriert sind und berücksichtigt werden.
5. Kritische Safety-Systeme sollten überprüft und entsprechende Maßnahmen eingeleitet werden, um zu gewährleisten, dass die OT-Cybersecurity-Risiken im Rahmen eines Safety-Vorfalls regelmäßig evaluiert werden.

Einführung

Im Sommer 2018 führte das unabhängige Forschungs- und Analyseunternehmen Bloor Research gemeinsam mit TÜV Rheinland eine internationale Onlinebefragung von 370 Industrieunternehmen durch. Ziel der Umfrage war es, zu erfahren, wie Organisationen Probleme im Zusammenhang mit ihrer OT-Cybersecurity meistern.

Cybersecurity-Hacks und Angriffe auf elektromechanische und elektronische Systeme waren vor dem mittlerweile berüchtigten Angriff von Stuxnet auf iranische Atomanlagen, der 2010 bekannt gemacht wurde, relativ unbekannt (Zetter, 2014). Dieser jetzt als OT bezeichnete Bereich, zu dem die Hardware und Software zählen, mit der durch die direkte Überwachung und / oder Steuerung physischer Geräte Änderungen an physikalischen Prozessen erkannt oder hervorgerufen werden, hat die verstärkte Aufmerksamkeit von Hackern und Angreifern erregt. Der vorliegende Ausblick auf 2019 wurde mit dem Ziel verfasst, Ansätze zum Management und zum Schutz von OT-Systemen in verschiedenen Branchen zu betrachten und aktuelle Ansichten zu Fragen der OT-Cybersecurity zu beleuchten.

ABBILDUNG 1:
In welcher Branche sind Sie hauptsächlich tätig?



In diesem Bericht wird untersucht, wie Organisationen in verschiedenen Bereichen der Industrie die Bedrohung von OT-Systemen beurteilen und welche Anstrengungen dagegen unternommen werden. Der Rahmen basiert auf dem vom US-amerikanischen National Institute of Standards und Technology (NIST) entwickelten Konzept zur Verbesserung der Cybersecurity kritischer Infrastrukturen „Framework for Improving Critical Infrastructure Cybersecurity“ (Version 1.1 vom 16. April 2018).

Die Befragten entschieden sich eigenständig für eine Teilnahme und es gab keine spezifischen Zielgruppen im Hinblick auf Organisationen oder Branchen, da die Umfrage auf alle OT-Bereiche ausgerichtet war. Die meisten Befragten kamen aus der Produktion. Einige Fragen der Umfrage waren zwangsläufig allgemeiner gehalten. Zum Beispiel hätte unter den Begriff „Risikobewertung“ auch eine „Überprüfung der Kontrollen“ fallen können, so dass die Umfrageergebnisse hätten verschieden ausgelegt werden können. Bei dieser Art von Umfrage ist es nicht möglich, ausführliche Details von jedem einzelnen Befragten zu erfassen. Daher konzentriert sich dieser Bericht auf die Grundaussage jeder Antwort, um gültige Daten zu erfassen und die wichtigsten Erkenntnisse hervorzuheben.

ABBILDUNG 2:
Welche Stellenbezeichnung beschreibt Ihre Position/Rolle am besten?

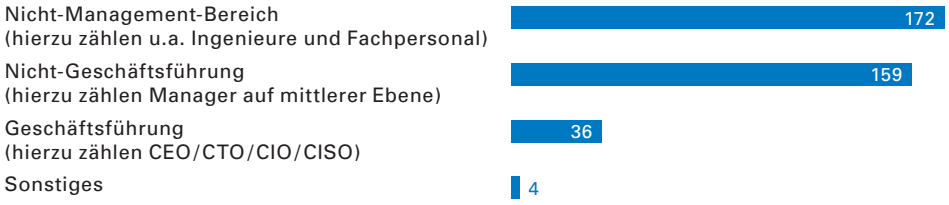
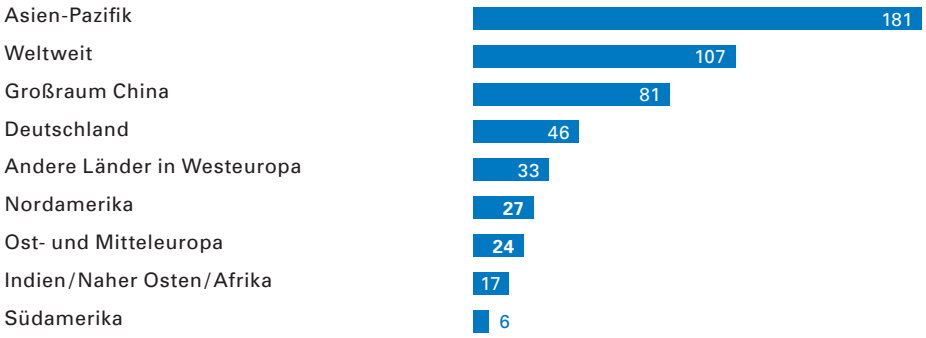


ABBILDUNG 3:
Für welche Region(en) sind Sie in erster Linie verantwortlich? (Multiple Choice)



Die Bedeutung von Risikobewertungen für OT-Systeme

Die meisten etablierten Unternehmen haben ein gutes Verständnis ihres Risikoprofils. Dies kann verschiedene Aspekte umfassen – von den Auswirkungen geopolitischer Faktoren über die Unsicherheit der Finanzmärkte bis hin zum Mangel an für den Herstellungsprozess kritischen Rohstoffen.

Risiken im Zusammenhang mit Informationssicherheit oder Cybersecurity werden zunehmend in das Risikoregister von Unternehmen aufgenommen, da sich Führungskräfte dieser Probleme immer mehr bewusst werden. Dieses bessere Verständnis wird von vielen angesehenen internationalen Gremien wie z. B. dem Weltwirtschaftsforum unterstützt, die Cybersecurity als ein wichtiges Element in ihre Analysen von Bedrohungen und Risiken aufgenommen haben (Weltwirtschaftsforum, 2018).

2018 – Analyse, Fakten und Zahlen

Bei der Diskussion über Risiken ist es wichtig zu verstehen, wie sich IT-Sicherheit und OT-Cybersecurity unterscheiden.

Die Informationstechnologie in Unternehmen ist so strukturiert, dass die Vertraulichkeit der Daten gewahrt wird. Es werden Maßnahmen getroffen, die den Schutz der Integrität und der Verfügbarkeit der Systeme gewährleisten.

In vielen Organisationen ist Verfügbarkeit vermutlich kein großes Geschäftsrisiko. Wenn E-Mails zehn Minuten verspätet sind, können viele Organisationen trotzdem funktionieren und das Geschäftsergebnis wird dadurch nicht beeinträchtigt. Es gibt natürlich Ausnahmen, aber für viele Unternehmen ist eine derartige Verzögerung kein Problem.

IT-Systeme von Unternehmen haben nur eine begrenzte Lebensdauer. Da die Hardware im Einklang mit dem Moore-Gesetz (Intel Corporation, 2018) ständig verbessert wird, wird Computerhardware etwa alle 2–3 Jahre ausgewechselt. IT-Systeme sollten regelmäßig gepatcht werden und Updates erhalten, da ständig neue Bedrohungen auftauchen und Anbieter anfällige Software schnell patchen wollen. In vielen Fällen ist dieser Patch-Zyklus sehr viel einfacher als früher, da Unternehmen die Notwendigkeit verstehen, Patches innerhalb kurzer Zeit zu testen und anzuwenden und weil Anbieter regelmäßig und verlässlich Patches herausbringen.

Das Risikoprofil von OT und industriellen Steuerungssystemen unterscheidet sich oft von dem gängiger IT-Systeme. Daher muss bei diesen Systemen ein anderer Ansatz zur Anwendung kommen.

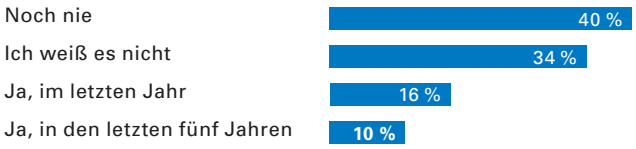
Die Lebensdauer von OT-Systemen kann oft mehr als das Zehnfache der Lebensdauer des IT-Systems eines Unternehmens betragen. Während seiner Lebensdauer wird ein Steuerungssystem, wenn überhaupt, vermutlich nur selten aktualisiert oder gepatcht. Dies steht im krassen Gegensatz zu der scheinbar unendlichen Summe von Patches, die für ein IT-System benötigt werden.

Die zunehmende Anzahl von OT-Systemen, die mit dem Internet verbunden sind, stellt den traditionellen Regelungstechniker vor eine Herausforderung. Ein Unternehmen oder ein Hersteller von OT-Systemen drängt eventuell darauf, ans Netz angeschlossene Geräte oder industrielle IoT-Geräte (Maw, 2018) zu nutzen. Damit sollen Kosten gesenkt werden, z. B. durch vorbeugende Instandhaltung. Diese Strategie findet dagegen in einer Betriebsumgebung, in der man sich der Cybersecurity-Risiken bewusst ist, nur wenig Beachtung. Die Vorstellung, Geräte und Systeme standardmäßig und ohne strikte Sicherheitsmaßnahmen an das Internet anzuschließen, geht für viele erfahrene OT-Cybersecurity-Fachleute verständlicherweise einen Schritt zu weit.

Funktionale Sicherheit, die direkt mit der menschlichen Sicherheit verknüpft ist, sollte das oberste Ziel eines jeden OT-Systems sein. Einsatzfähigkeit ist in der Regel von entscheidender Bedeutung für den Geschäftsbetrieb. Die Notwendigkeit zu gewährleisten, dass eine Anlage weiter in Betrieb ist, ist in der Regel das zweite Ziel, gleich nach den Sicherheitsanforderungen. Jede Ausfallzeit eines Systems kann erhebliche Kosten verursachen. In einer angespannten Wirtschaftslage kann dies den Unterschied zwischen Gewinn und finanziellen Verlusten bedeuten.

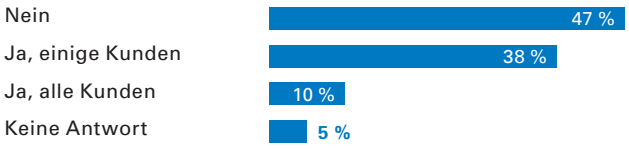
Die Antworten auf unsere nächste Frage ergaben, dass 40 % der Befragten noch nie eine Risikobewertung ihrer OT-Systeme durchgeführt hatten. 34 % der Befragten wussten nicht, ob eine Risikobewertung durchgeführt wurde.

ABBILDUNG 4:
Haben Sie schon einmal eine OT-Risikobewertung durchgeführt?



Unternehmen, die Aufträge an Hersteller oder Industriezulieferer vergeben, wollen zunehmend sichergehen, dass OT-Cybersecurity-Risiken berücksichtigt werden. Aufträge werden nur dann erteilt, wenn die Gewissheit besteht, dass geistiges Eigentum, wie z. B. CAD-Zeichnungen, vom Hersteller geschützt wird. In der Automobilindustrie gibt es hierzu bereits ein eigenes Assessment, TISAX (www.enx.com/TISAX).

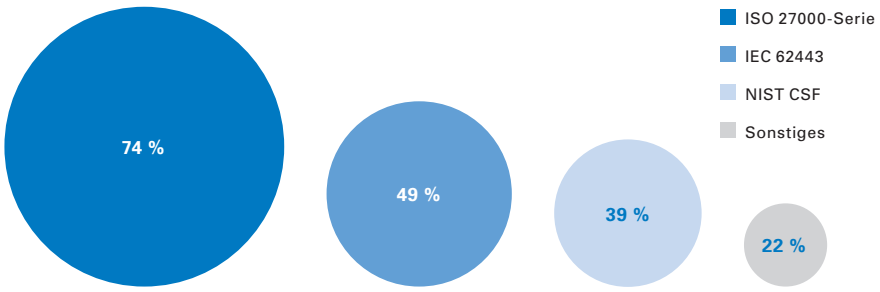
ABBILDUNG 5:
Verlangen Ihre Kunden von Ihnen ausdrücklich einen Nachweis, dass Sie Schritte unternommen haben, um Ihr OT-Netzwerk zu sichern?



Von den Befragten gaben 38% an, dass einige oder alle ihrer Kunden einen Nachweis der Sicherheit des OT-Netzwerks verlangen. Obwohl 47% der Befragten sagten, dass ihnen diese Frage noch nicht gestellt worden sei, besteht unweigerlich eine Nachfrage nach einem Supply-Chain-Risikomanagement. Es wird erwartet, dass immer mehr Hersteller und Industriezulieferer den Nachweis erbringen müssen, dass Cybersecurity-Risiken für OT-Systeme ausgeschaltet wurden. Diese Anforderung wird aufgrund der steigenden Nachfrage Auswirkungen auf die Budgets und Investitionen in OT-Cybersecurity-Maßnahmen haben.

Ein häufig angewendeter Information-Security-Management System-Standard (ISMS) ist die ISO/IEC-27000-Serie. Dieser umfassende Satz von Standards bildet den Grundstein für die Informationssicherheit von IT-Systemen. Mit dem Aufkommen neuer Rahmenkonzepte zur Bewertung von OT wird sich der Einsatz dieser Standards bei der Bewältigung derartiger Cybersecurity-Risiken wahrscheinlich verringern. Diese Serie wurde von 74% der Befragten verwendet. 49% der Befragten verwendeten die ANSI/IEC-62443-Serie (Abbildung 6).

ABBILDUNG 6:
Welche Rahmenwerke oder Standards haben Sie für die Bewertung [von Cybersecurity-Risiken] verwendet? (Mehrere Antworten möglich)



Das ist eine Reihe von Standards des American National Standards Institute und der International Electrotechnical Commission, in denen Verfahren zur Implementierung von Cybersecurity für industrielle Automatisierungs- und Steuerungssysteme (IEC) festgelegt werden. Diese Standards wurden ursprünglich als ANSI/ISA-99- oder ISA99-Standards bezeichnet.

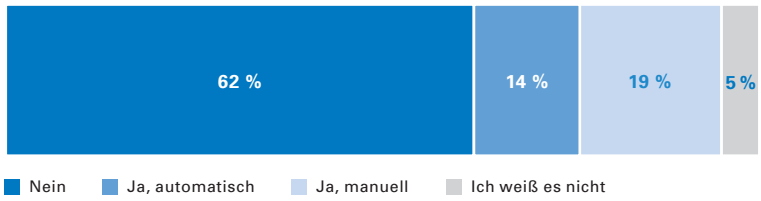
39% der Befragten nutzten das vom National Institute of Standards and Technology (NIST) herausgegebene Rahmenkonzept zur Verbesserung der Cybersecurity kritischer Infrastrukturen. Dieses Rahmenkonzept wurde ursprünglich für den Betrieb kritischer Infrastrukturen entwickelt, wird jedoch von einer Vielzahl von Organisationen verwendet. Es soll Organisationen bei der Bewertung und Verbesserung ihrer Fähigkeit helfen, Sicherheitsvorfälle zu verhindern, zu erkennen und auf sie zu reagieren.

Andere als die oben genannten Regularien wurden von 22% der Befragten angeführt. In vielen Fällen waren die Regelungen sehr branchenspezifisch. Zu diesen Regularien zählen SAE J3061, JASO TP15002, ISO26262, Druckgeräterichtlinie, IATF16949, MIL-STD-882D, NCIIPC und C2M2. Nicht alle dieser Standards sind auf Bewertungen allgemeiner OT-Cybersecurity-Risiken anwendbar.

Einige Organisationen haben für diese Aufgabe mehrere Standards gewählt. Dieser Syntheseansatz kommt immer häufiger zum Einsatz, da einzelne Standards möglicherweise nicht alle wahrgenommenen Risiken oder Probleme eines Unternehmens abdecken. Dies spiegelt sich auch in der Tatsache wider, dass sowohl das NIST-Rahmenwerk zur Verbesserung der Cybersecurity kritischer Infrastrukturen als auch die IEC-62443-Serie andere Standards für ihren Ansatz heranziehen.

Von den Befragten konnten 62% nicht alle OT-Assets erkennen, und nur 14% verfügten über eine Form der automatischen Endpunkterkennung.

ABBILDUNG 7:
Sind Sie in der Lage, alle Endpunkte in Ihrem OT-Netzwerk zu erkennen?



OT-Cybersecurity-Risiken werden selten als separate Risiken gesehen. Häufig werden sie in das IT-Gesamtrisiko miteinbezogen oder aufgrund ihres Einflusses auf den Produktivitätsverlust sogar als Teil des Produktionsrisikos betrachtet. Darüber hinaus ist die OT-Ausstattung mitunter schwer zu verfolgen, da die seriellen Netzwerke, die im Laufe der Jahre angeschafft und erweitert wurden, um der wachsenden Produktionsnachfrage Rechnung zu tragen, oft unzureichend dokumentiert sind.

Ausblick 2019 – Maßnahmen

MANAGEMENT

- Behandeln Sie das OT-Cybersecurity-Risiko als separaten handlungsbedürftigen Posten in Ihrem Budget. Mit der zunehmenden Fokussierung von Hacker-Aktivitäten auf OT ist es von entscheidender Bedeutung, dass Ihr Unternehmen dieser Bedrohung mit Nachdruck begegnet.

OT-VERANTWORTLICHE

- Kennen Sie Ihr Risiko und schränken Sie es durch die Anwendung geeigneter Rahmenbedingungen und Werkzeugen ein. Ziehen Sie den Einsatz von Produkten zur automatischen Erkennung von OT-Komponenten in Betracht und wählen Sie eine nichtinvasive „sanfte“ Herangehensweise, die das OT-Netzwerk nicht stört, und den Netzwerkverkehr nicht erhöht und daher die Systemleistung nicht beeinträchtigt.

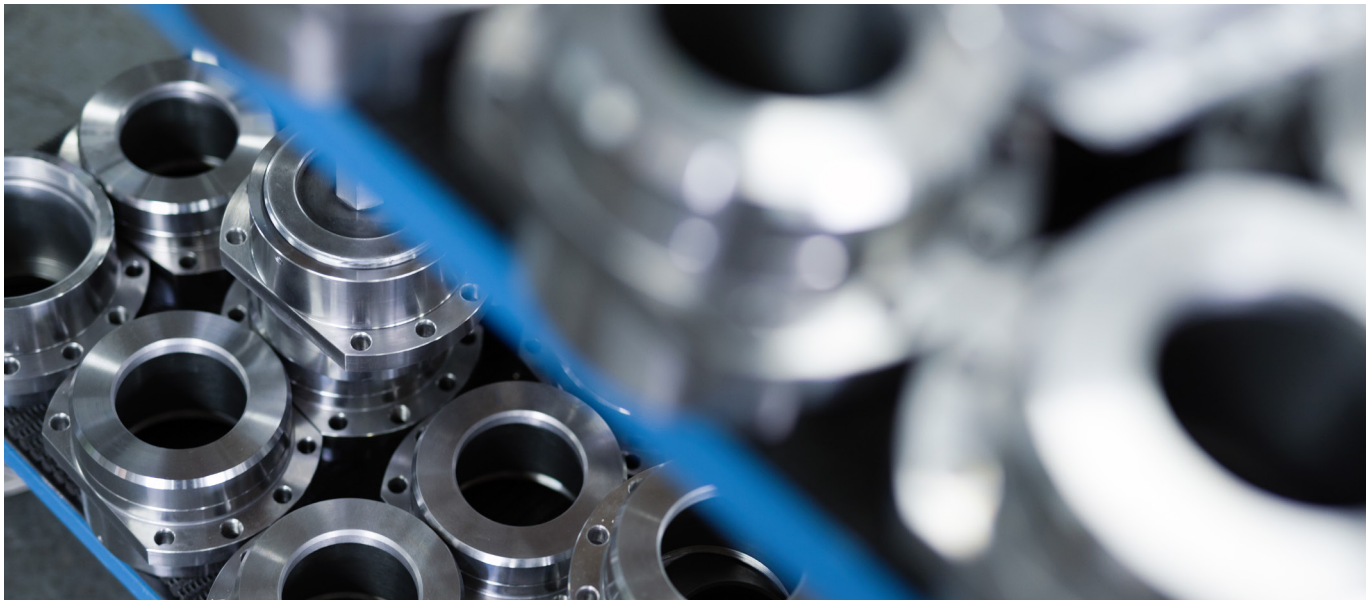
Schutz von OT-Anlagen vor Cyber-Bedrohungen

Wir haben gesehen, dass das Verständnis und die Begrenzung der Risiken von OT-Systemen der erste Schritt bei der Problembewältigung sind. OT-Systeme müssen durch eine Kombination aus Richtlinien und Verfahren, technischen Kontrollen, Benutzeraufklärung und unterstützenden Prozessen geschützt werden.

2018 – Analyse, Fakten und Zahlen

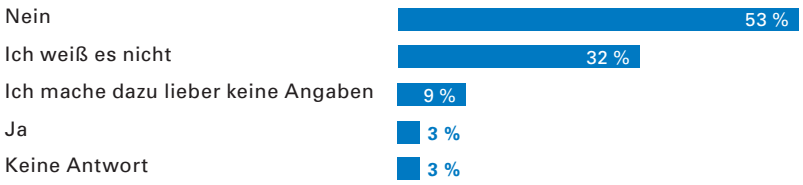
ABBILDUNG 8:
Haben Sie OT-spezifische Cybersecurity-Richtlinien und -Verfahren in Ihrem Unternehmen implementiert?

Von den Befragten haben 43% keine Richtlinien und Verfahren für ihre OT-Systeme, und 31% verlassen sich auf die (vermutlich allgemeineren) Richtlinien und Verfahren, die von ihrer IT-Abteilung erstellt wurden.



Für OT-Systeme müssen Richtlinien und Verfahren existieren, die speziell an diese Umgebung angepasst wurden. 20% der Befragten haben derartige Richtlinien und Verfahren implementiert. Natürlich können viele IT-Richtlinien auf das OT-Umfeld angewendet oder entsprechend angepasst werden. Die bewusste Einführung von OT-spezifischen Richtlinien und Verfahren ist jedoch wichtig.

ABBILDUNG 9:
Haben Sie im letzten Jahr aufgrund von Datendiebstahl OT-bezogenes geistiges Eigentum verloren?



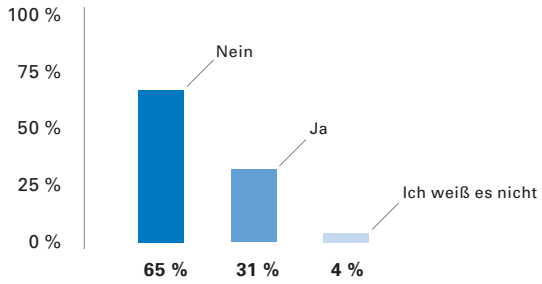
Es ist interessant, dass 53% der Befragten sagen konnten, dass sie im letzten Jahr kein OT-bezogenes geistiges Eigentum verloren haben. Wie erwartet, wollten sich einige der Befragten dazu nicht äußern. Obwohl es sich hier um eine anonyme Umfrage handelte, ist der Verlust von Daten ein sensibles Thema. Es ist daher verständlich, dass man darüber in der Öffentlichkeit nicht sprechen möchte.

Die Verantwortung für die physische Sicherheit der Systeme fällt häufig in den Zuständigkeitsbereich des Gebäudemanagement-Teams und nicht in den eines für die Cybersecurity verantwortlichen Teams (IT oder OT). Bei OT-Anlagen spiegelt sich die Tatsache, dass die physische Sicherheit häufig von einem für die Gebäudeverwaltung zuständigen Team und nicht von einer IT-Gruppe verwaltet wird, darin wider, dass die meisten Befragten (78%) nicht für die physische Sicherheit verantwortlich waren. Die 20% der OT-Cybersecurity-Teams, die auch für die physische Sicherheit verantwortlich sind, weisen klar den Weg zu konvergenten Sicherheitslösungen (Abbildung 10).

ABBILDUNG 10:
Sind Sie für die physische Sicherheit Ihrer Anlage(n), Systeme oder Prozessnetzwerke verantwortlich?

In dieser Umfrage gaben 31 % der Befragten an, dass sie ein spezielles Schulungs- und Weiterbildungsprogramm für OT-Cybersecurity haben. 65 % der Befragten sind auf ihre derzeit existierenden Schulungen zur Informationssicherheit angewiesen.

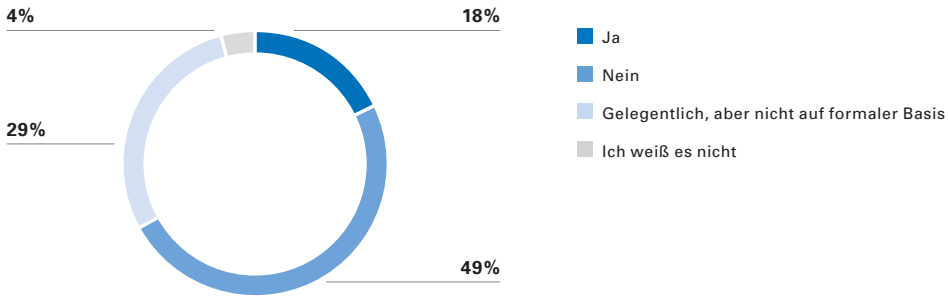
ABBILDUNG 11:
Haben Sie ein spezielles Schulungs- und Weiterbildungsprogramm für OT-Cybersecurity?



Das Teilen von Informationen zu OT-Bedrohungen ist ein neues Konzept. Viele Organisationen fangen gerade erst an, sich ein Bild von ihrem OT-Risiko und dem damit verbundenen Bewusstsein für die Situation zu machen. Beides sind wichtige Voraussetzungen für die Entwicklung eines betriebsinternen „Intelligence Models". Sobald ein Modell geschaffen wurde, kann überlegt werden, wie dieses mit anderen Unternehmen in der Branche geteilt werden kann.

Von den Befragten gaben 49 % an, Informationen über OT-Bedrohungen nicht aktiv mit anderen Unternehmen in der Branche zu teilen. Nur 18 % tun dies auf formaler Basis.

ABBILDUNG 12:
Teilen Sie Informationen zu OT-Bedrohungen aktiv mit anderen Unternehmen in der Branche?



Für kritische Infrastrukturen kann dieser Informationsaustausch durch die Mitwirkung der Regierung oder von Aufsichtsbehörden beschleunigt werden, da Systeme und Prozesse von zentraler und nationaler Bedeutung unbedingt geschützt werden müssen. Es wird erwartet, dass der Austausch von OT-Informationen zunehmen wird, sobald der damit verbundene Nutzen erkennbar ist.

Ausblick 2019 – Maßnahmen

MANAGEMENT

- Sorgen Sie dafür, dass es in Ihrem Unternehmen eine Kultur des Schutzes von OT-relevanten Daten gibt. In vielen Fällen kann der Verlust von OT-Daten vertrauliche Geschäftsinformationen Ihres Unternehmens offenbaren. Diese Daten können vieles umfassen, von der Produktionsleistung bis zum Verhältnis von Komponenten bei der Herstellung eines Produkts – all das ist für Wettbewerber von großem Interesse. Unterstützen Sie Maßnahmen zur Verhinderung von Datendiebstahl.
- Gewährleisten Sie, dass es in Ihrem Unternehmen ein Schulungsprogramm für OT-Cybersecurity gibt. Viele Organisationen bieten IT-Cybersecurity-Schulungen für ihre Mitarbeiter an. Eine gut informierte Belegschaft kann Auge und Ohr eines Informationssicherheitsprogramms sein und Probleme wie Phishing-E-Mails und den Missbrauch von USB-Sticks oder ähnlichen Datenspeichern erkennen und entsprechend handeln. Diese Schulungen sollten auf OT-Cybersecurity ausgedehnt werden.

OT-VERANTWORTLICHE

- Denken Sie auch an die physische Sicherheit. Der Trend zu einer Konvergenz der Sicherheit nimmt zu, d. h. die logische Sicherheit (IT oder OT) und die physische Sicherheit fallen in einen einzigen Zuständigkeitsbereich. Dies ist in vielen Organisationen sehr sinnvoll, da die physische Sicherheit von OT-Anlagen kritisch ist. Wenn der physische Zugriff auf eine Produktionsstätte oder Fabrik verhindert wird, können das Platzieren von Implantaten durch Angreifer sowie direkter Diebstahl vermieden werden. Das Erkennen eines physischen Sicherheitsereignisses oder -vorfalls und das Ergreifen entsprechender Maßnahmen können einen damit zusammenhängenden logischen Angriff auf OT-Systeme verhindern.
- Binden Sie alle Mitarbeiter in Ihr Cybersecurity-Schulungsprogramm ein. Schulungen und Weiterbildungen für OT-Cybersecurity müssen an die Bedürfnisse der beteiligten Teams aus allen Bereichen des Unternehmens angepasst werden. Das schließt auch die Mitarbeiter aus der Produktion und der Geschäftsleitung ein.
- Teilen Sie Informationen zu Cyber-Bedrohungen und nutzen Sie diese Informationen, um Ihr Unternehmen und andere in Ihrer Branche zu schützen. Das Teilen von Informationen über Bedrohungen ist jetzt in vielen Branchen üblich, da die Wettbewerber zunehmend den Nutzen erkennen, den ein Austausch von Erkenntnissen zu Problemstellen dem Schutz der Gemeinschaft bringt. Es gibt natürlich die Erwartung einer Gegenseitigkeit und die Hoffnung, dass ein Wettbewerber Informationen liefern kann, die konkurrierenden Unternehmen helfen könnten, Bedrohungen und Schäden zu vermeiden. Unabhängig davon ist ein solcher Informationsaustausch für jeden OT-Sektor von Vorteil.

Erkennung von OT-Cybersecurity-Vorfällen

Überwachungslösungen für IT-Netzwerke werden seit vielen Jahren eingesetzt, und die meisten Unternehmen, die innerbetriebliche IT-Systeme betreiben, verfügen über ein System zum Überwachen und Erkennen von Cyber-Bedrohungen.

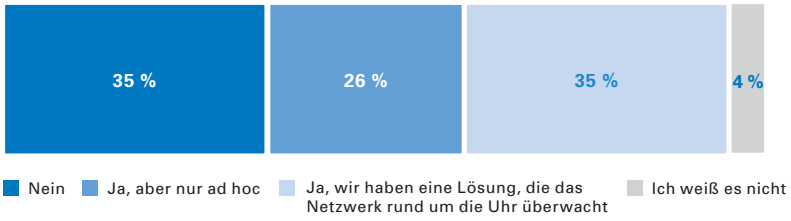
Die OT-Netzwerküberwachungsbranche hat in den letzten Jahren einen starken Boom erlebt. Eine Reihe von Anbietern bietet Produkte an, die OT-Komponenten erkennen und OT-Netzwerke überwachen, um Cyber-Bedrohungen aufzuspüren. Ein wichtiges Verkaufsargument für viele dieser Lösungen ist, dass sie passiv sind und nur den Netzwerkverkehr und die Kommunikation zwischen den OT-Komponenten überwachen. Dieser Ansatz vermeidet aggressivere und aktivere Netzwerkscans, die die Leistung und Stabilität eines OT-Netzwerks beeinträchtigen könnten.

Das passive Scannen hat jedoch seine Grenzen und die umsichtige Anwendung eines aktiveren Ansatzes könnte zu deutlich besseren Scan-Ergebnissen führen. Die Zunahme verschlüsselter OT-Netzwerkprotokolle wird sich negativ auf das passive Scannen auswirken. Daher ist ein Übergang zu aktiveren Lösungen wahrscheinlich.

2018 – Analyse, Fakten und Zahlen

Es ist ein gutes Zeichen, dass 35% der Befragten über eine Lösung verfügen, die das OT-Netzwerk rund um die Uhr überwacht. Das bedeutet, dass ihr OT-Netzwerk die gleiche Transparenz wie ihr IT-Netzwerk aufweist.

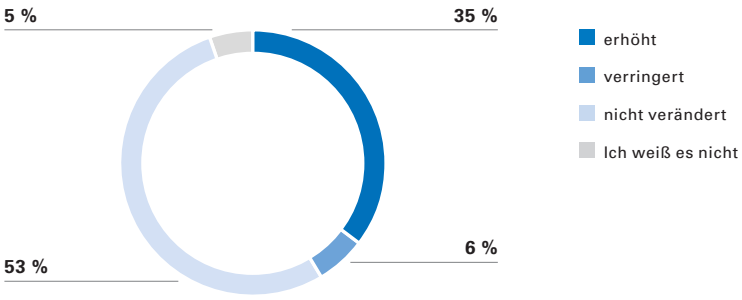
ABBILDUNG 13:
Überwachen Sie Ihr OT-Netzwerk kontinuierlich auf Cyber-Bedrohungen?



Mit Sicherheit wächst das Interesse, solche Systeme anzugreifen, entweder durch „Hacktivisten", Hacker oder staatliche Akteure. In den Medien gibt es regelmäßig Berichte über gehackte OT-Systeme, und die Berichterstattung ist zum Teil dramatisch und aufsehenerregend (Corera, 2017).

Eingehende Bedrohungen von OT-Systemen werden daher mit der Zeit wahrscheinlich zunehmen. Umso wichtiger ist es, dass eine Organisation in der Lage ist, Bedrohungen überhaupt zu erkennen. Die meisten Verfahren zur Analyse von Cyber-Bedrohungen umfassen mehrere Schritte. Zunächst wird ein Rahmen festgelegt, der definiert, welche Informationen erforderlich sind, um Bedrohungen besser zu verstehen. Gibt es beispielsweise eine bestimmte speicherprogrammierbare Steuerung, die in einer Anlage eingesetzt wird? Wenn ja, könnte diese ein Ziel von Angriffen sein. Anschließend können Daten zu Bedrohungen aus verschiedenen Quellen gesammelt werden, einschließlich öffentlich zugänglicher Informationen aus Sicherheitsforen der Industrie und der Regierung sowie aus Datenbanken von Produktanbietern. Diese Daten müssen dann analysiert werden, um weitere Informationen zu den Auswirkungen auf das Geschäftsrisiko zu erhalten.

ABBILDUNG 14:
Hat sich die Anzahl der OT-spezifischen Cybersecurity-Bedrohungen auf Ihr Unternehmen im vergangenen Jahr ...



Diese Analyse der Cyber-Bedrohungen von OT-Systemen könnte eine bedeutende Änderung in der Art und Weise darstellen, wie einige Organisationen ihr Risiko hinsichtlich der Prozesssteuerung managen. Es ist nicht überraschend, dass 35 % der Befragten erwarteten, dass derartige OT-Cyber-Bedrohungen zunehmen. Dieser Trend spiegelt möglicherweise ein größeres Bewusstsein und den Einsatz besserer Nachweismethoden wider. Wenn 53% der Befragten der Meinung waren, dass die Anzahl der Bedrohungen gleich bleibt, bedeutet dies zumindest, dass sie diese Bedrohungen verfolgen und aufzeichnen.

Ausblick 2019 – Maßnahmen

MANAGEMENT

- Sie müssen verstehen, dass Ihr Unternehmen ein Angriffsziel für OT-Cybersecurity-Bedrohungen ist und dass Sie diese Bedrohungen erkennen und bekämpfen müssen. Im Gegensatz zu Safety-Bedrohungen entwickeln und verändern sich Cybersecurity-Bedrohungen kontinuierlich weiter. In diesem Zusammenhang wird eine Bedrohung als all das definiert, was eine Schwachstelle angreifen kann (z.B. ein Softwarefehler) und die Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems beeinträchtigen kann.

OT-VERANTWORTLICHE

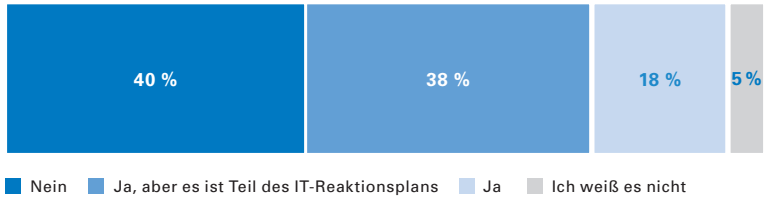
- Machen Sie sich ein vollständiges Bild von den OT-Bedrohungen. Es kann kompliziert sein, unterschiedliche Daten zusammenzufügen, um verwertbare Informationen über Bedrohungen zu erlangen. Das kann jedoch dazu beitragen, Bereiche zu identifizieren, in denen das Unternehmen Maßnahmen ergreifen muss. Das ist die letzte Phase des Prozesses. Nur durch die effektive Verarbeitung von Daten über Bedrohungen können kostengünstige und angemessene Maßnahmen zum Schutz von OT-Anlagen getroffen werden.

Ergreifen von Maßnahmen nach einem OT-Cybersecurity-Vorfall

Sobald ein Ereignis oder ein Vorfall entdeckt wurde, muss eine angemessene Reaktion eingeleitet werden. Dabei ist ein gut eingespielter Reaktionsplan von entscheidender Bedeutung. Auch wenn ein Computernetz bisher noch nicht angegriffen wurde, besteht eine hohe Wahrscheinlichkeit, dass es in Zukunft einen Angriff erleben wird. In den Reaktionsplänen von Unternehmen werden OT-Systeme häufig ausgelassen, was sie bei einem Cyberangriff teuer zu stehen kommen kann.

2018 – Analyse, Fakten und Zahlen

ABBILDUNG 15:
Haben Sie ein spezielles Verfahren zur Reaktion auf OT-Zwischenfälle oder Vorfälle im Zusammenhang mit Industrial Security?



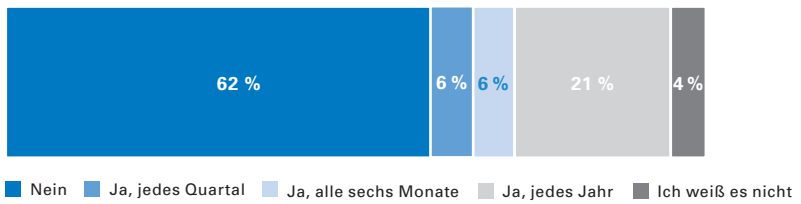
Ein separater OT-spezifischer Reaktionsplan ist ideal. Falls dieser jedoch Teil des IT-Reaktionsplans ist, wie es von 38% der Befragten angegeben wurde, ist dies häufig ausreichend, solange spezifische OT-Probleme identifiziert und behoben werden. Die anfängliche Reaktionszeit ist vergleichbar mit der sogenannten „goldenen Stunde" in der Akutversorgung von Patienten, wobei der Zustand eines Patienten entscheidend verbessert werden kann, wenn innerhalb einer Stunde nach einem Unfall oder einer Verletzung ein wirksamer Behandlungsplan aufgestellt wird. In der ersten Phase der Reaktion auf einen OT-Vorfall müssen die wichtigsten Teammitglieder zusammengebracht werden, damit schnell eine effektive Strategie festgelegt werden kann, mit der man auf Grundlage der vorherigen Planung und Übungen auf den Vorfall zu reagieren kann.

Die Einbindung anderer Fachleute, z. B. aus der Personalabteilung, Öffentlichkeitsarbeit und der Rechtsabteilung, kann die Arbeitslast verteilen und gewährleistet außerdem, dass Probleme außerhalb der technischen Systeme frühzeitig angegangen werden. Dazu zählen das Management des Personals, die Art und Weise der Verbreitung von internen/externen Meldungen und die Ermittlung des Rechtsrahmens für den Vorfall und den Wiederherstellungsprozess. Von den Befragten hatten 44 % einen Plan, andere Fachkräfte bei Vorfällen einzubinden.

ABBILDUNG 16:
Bezieht Ihr Reaktionsplan andere Fachleute, wie Personalabteilung, Öffentlichkeitsarbeit und Rechtsabteilung, mit ein?

Wie regelmäßig ein OT-Reaktionsplan geübt werden muss, hängt sehr stark von der Art des Geschäfts der jeweiligen Organisation ab. Die richtige Antwort ist: so oft wie nötig. Auf jeden Fall sollte eine jährliche Übung die Norm sein. Daher ist es besorgniserregend, dass 62% der Befragten den OT-Reaktionsplan nicht regelmäßig durchgehen. Wenn im Ernstfall auf einen Vorfall reagiert werden muss, führt mangelnde Übung zu größeren Problemen.

ABBILDUNG 17:
Führen Sie regelmäßig Übungen Ihres OT-Reaktionsplans aus?



Ausblick 2019 – Maßnahmen

MANAGEMENT

- Sorgen Sie dafür, dass Ihr Unternehmen einen wirksamen und gut eingespielten Reaktionsplan für OT-Vorfälle hat.

OT-VERANTWORTLICHE

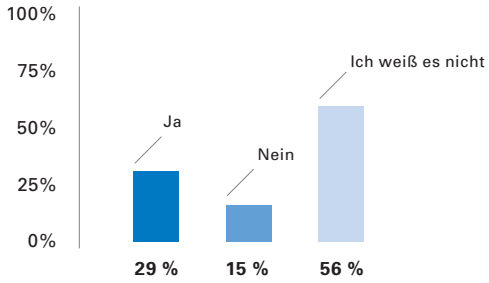
- Üben Sie regelmäßig Ihren Reaktionsplan für OT-Vorfälle. Wie oft Sie üben, hängt von der Art der Geschäfte Ihres Unternehmens und den damit verbundenen Risiken ab.
- Bauen Sie ein interdisziplinäres Team auf, um auf OT-Cybersecurity-Bedrohungen zu reagieren. Die Art der Beratung durch Personalabteilung, Öffentlichkeitsarbeit und Rechtsabteilung unterscheidet sich bei Vorfällen/in Krisenfällen häufig von der im Alltagsgeschäft üblichen: Ermitteln Sie frühzeitig, wer diesen speziellen Beitrag leisten kann.

Wiederherstellung des Geschäftsbetriebs nach einem OT-Cybersecurity-Vorfall

Sobald ein Vorfall behoben wurde und keine Gefahr für weitere Störungen oder Schäden besteht, muss ein Wiederherstellungsprozess eingeleitet werden, um den Geschäftsbetrieb wie gewohnt fortsetzen zu können. Dieser Prozess umfasst oftmals den Wiederaufbau und die Neukonfiguration von OT-Hardware und -Software.

2018 – Analyse, Fakten und Zahlen

ABBILDUNG 18:
Existieren Pläne zur Wiederherstellung des Betriebs nach einem OT-Cybersecurity-Vorfall?



Es wurde festgestellt, dass nur 29% der Befragten einen Plan hatten, um die Geschäftsprozesse nach einem Vorfall im Zusammenhang mit OT-Cybersecurity wiederherzustellen. Die 15% der Befragten, die nicht über einen derartigen Plan verfügten, müssten nach einem schwerwiegenden Vorfall wahrscheinlich mit erheblichen Problemen bei ihren Betriebsabläufen rechnen.

Ausblick 2019 – Maßnahmen

MANAGEMENT

- Sorgen Sie dafür, dass ein formeller Plan zur Wiederherstellung des Betriebs existiert. Das ist fast so wichtig wie ein Reaktionsplan für OT-Vorfälle.

OT-VERANTWORTLICHE

- Stellen Sie sicher, dass Sie in der Lage sind, den Wiederaufbau Ihrer OT-Systeme zu unterstützen. Der Wiederherstellungsplan sollte Anweisungen enthalten, wie OT-Geräte zurückgesetzt, neu programmiert und neu konfiguriert werden können, einschließlich der entsprechenden Downloads/Uploads von Steuerungssoftware und der Einstellungen. Ohne einen spezifischen Plan sind OT-Systemkonfigurationen wahrscheinlich nicht Teil des Backups der OT-Systeme.

Budgets und OT-Cybersecurity

Budgets spielen eine große Rolle, wenn es darum geht, welche Prozesse, Verfahren und Kontrollen implementiert werden können, um eine OT-Anlage zu sichern. OT-Komponenten und -Systeme können sich in von der IT-Abteilung getrennten Bereichen befinden (z. B. Produktion, Gebäudemanagement oder Wartung). Daher sind die OT-Cybersecurity-Budgets möglicherweise breit gestreut, was ein größeres Risiko darstellen kann.

Wenn ein OT-Cybersecurity-Budget in das allgemeine IT-Cybersecurity-Budget integriert ist, stehen möglicherweise nicht alle für die Sicherung der OT-Umgebung erforderlichen Gelder zur Verfügung.
Ein unzureichendes Budget ist häufig eine Folge von interner Firmenpolitik oder hat seine Ursache darin, dass IT-Teams die Anforderungen an die digitale Absicherung einer OT-Einrichtung nicht richtig verstehen.

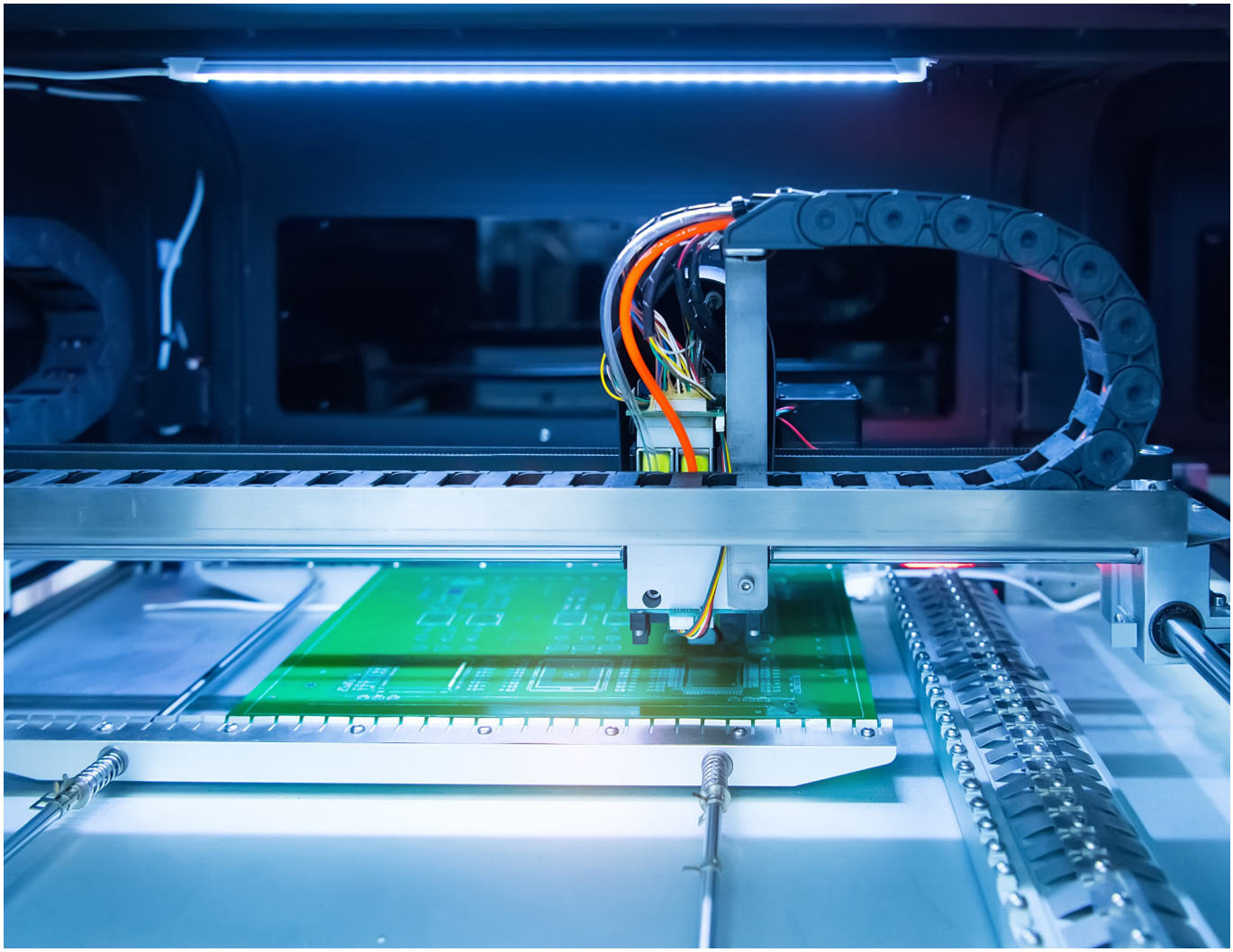
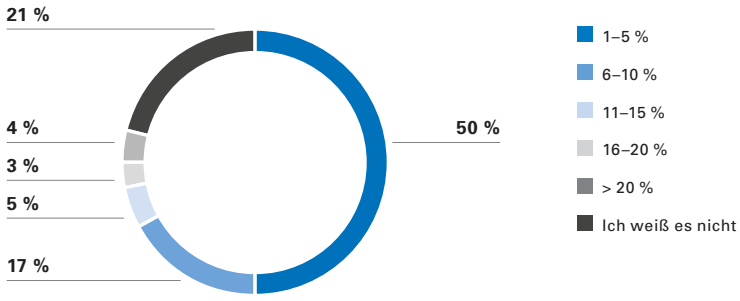
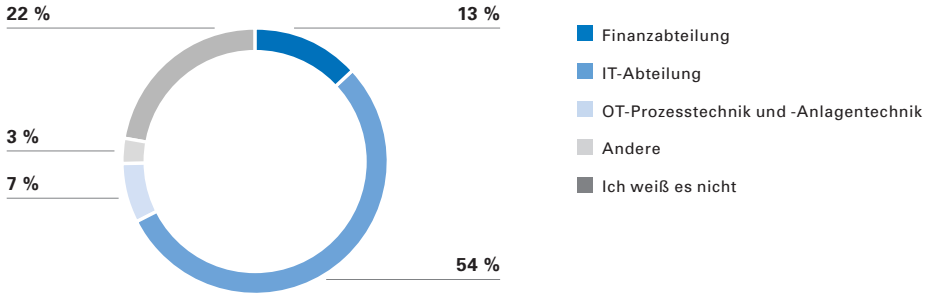


ABBILDUNG 19:
Welcher Prozentsatz Ihres IT-/OT-Budgets ist speziell für OT-Cybersecurity vorgesehen? (Wählen Sie den am nächsten liegenden Wert.)



Es überrascht nicht, dass 54% der Befragten sagten, dass ihr OT-Cybersecurity-Budget von der IT-Abteilung verwaltet wird. Bei 13% war es Teil des Budgets der Finanzabteilung. OT-Prozesstechnik und -Anlagentechnik hatten nur bei 7% der Befragten die Kontrolle über das Budget (Abbildung 20).

ABBILDUNG 20:
Welche Abteilung kontrolliert das Budget für OT-Cybersecurity-Produkte und -Services in Ihrem Unternehmen?



Ausblick 2019 – Maßnahmen

MANAGEMENT

- Stellen Sie sicher, dass OT-Cybersecurity ein angemessenes Budget erhält. Es gibt vermutlich keinen idealen Prozentsatz für die Zuteilung von OT-Cybersecurity-Budgets. Das Budget muss jedoch ausreichen, um relevanten, im Zusammenhang mit OT stehenden Cybersecurity-Risiken gerecht zu werden.

OT-VERANTWORTLICHE

- Sie müssen dafür sorgen, dass die Budgets für OT-Cybersecurity von Stellen kontrolliert werden, die die Anforderungen an die OT-Cybersecurity wirklich verstehen. Der Trend, dass IT-Abteilungen die Kontrolle über OT-Cybersecurity-Budgets haben, wird in den kommenden Jahren vermutlich weiter zunehmen.

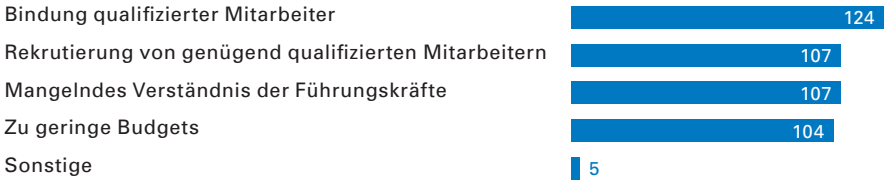
Besondere Anforderungen an OT-Cybersecurity

OT-Cybersecurity ist wohl eine der komplexesten Herausforderungen im OT-Bereich, da regelmäßig neue Bedrohungen auftauchen und die bestehenden Prozesssysteme mit der Bewältigung der wachsenden geschäftlichen Anforderungen konfrontiert werden.

Viele OT-Systeme sind seit Jahrzehnten im Einsatz und werden lediglich in einem Umfang gepflegt und gewartet, der ihre tägliche Betriebsbereitschaft gewährleistet. Andere OT-Systeme werden eingeführt, die zwar den Herausforderungen von Industrie 4.0 gerecht werden, aber die mit einem solchen stark vernetzten Konzept verbundenen Sicherheitsprobleme möglicherweise nicht bewältigen können (Industrie 4.0, 2018).

2018 – Analyse, Fakten und Zahlen

ABBILDUNG 21:
Welcher Bereich innerhalb Ihrer OT-Cybersecurity-Strategie stellt die komplexeste Herausforderung dar? (Multiple Choice)



Es ist ein gutes Zeichen, dass 31 % der Befragten sagen, dass ihr Führungsteam die Bedeutung von OT-Cybersecurity-Maßnahmen in vollem Umfang versteht. Es wird interessant sein, diesen Punkt im Laufe der nächsten Jahre weiter zu verfolgen, da es immer mehr Berichte über Hacker-Angriffe auf OT-Systeme gibt und das Bewusstsein für diese Schwachstellen geschärft wird.

ABBILDUNG 22:
Versteht Ihr Führungsteam die Bedeutung von OT-Cybersecurity-Maßnahmen in vollem Umfang?

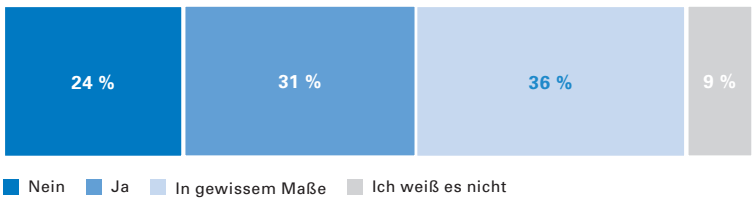
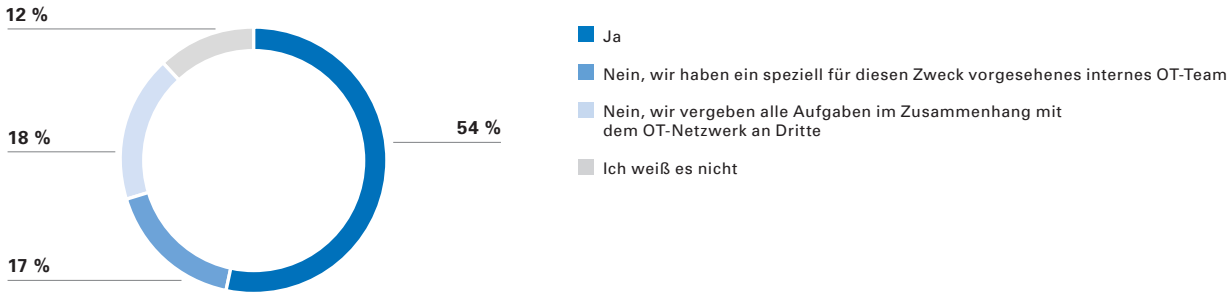
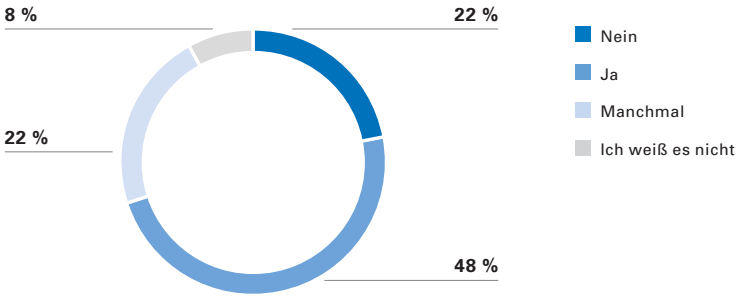


ABBILDUNG 23:
Ist Ihr IT-Team verantwortlich für das Management des OT-Netzwerks?



54% der Befragten gaben an, dass das IT-Team für die Verwaltung des OT-Netzwerks verantwortlich ist. 18% der Befragten konnte diese Aufgabe an externe Anbieter outsourcen. Diese Antwort spiegelt wahrscheinlich den Umstieg einiger Unternehmen auf Managed Services wider. 17% der Befragten verfügten über ein spezielles OT-Team, was für komplexere Umgebungen und Anlagen sinnvoll ist, für die ein derartiges Outsourcing schwierig wäre.

ABBILDUNG 24:
Beurteilen oder überprüfen Sie Fragen der Cybersecurity, wenn Sie sicherheitsrelevante Bewertungen durchführen?



In modernen Anlagen- und Prozessleitsystemen sind die funktionale Sicherheit und die Cybersecurity heutzutage untrennbar miteinander verbunden.

Funktionale Sicherheit ist die Absicherung gegen zufälliges und systematisches technisches Versagen zum Schutz von Leben und Umwelt. Cybersecurity dagegen ist die Abwehr von fahrlässigen und vorsätzlichen Handlungen zum Schutz von Geräten und Einrichtungen.

Selbst wenn eine Anlage streng auf funktionale Sicherheit ausgelegt ist, kann sie trotzdem anfällig für Cyberangriffe sein. Die Steuersysteme können gut konzipiert und implementiert sein – wenn jedoch eine HMI-Station (Mensch-Maschine-Schnittstelle) nicht durch grundlegende Sicherheitsmaßnahmen geschützt ist, kann es hier zu Manipulationen kommen.

48% der Befragten bewerteten oder überprüften Cybersecurity-Fragen im Rahmen von Safety-Bewertungen, 22 % hingegen taten dies nicht. Da immer mehr internationale Sicherheitsvorschriften verlangen, dass bei Safety-Beurteilungen auch Cybersecurity-Risiken bewertet werden, wird die Anzahl der Unternehmen, die im Rahmen ihrer Safety-Beurteilung keine Bewertung des Cybersecurity-Risikos durchführen, unvermeidlich zurückgehen.

Ausblick 2019 – Maßnahmen

MANAGEMENT

- Bauen Sie ein leistungsfähiges OT-Cybersecurity-Team auf, das Ihr Unternehmen gut unterstützen kann. Die Bindung qualifizierter Mitarbeiter, die sich gut mit Prozesstechnologien und Cybersecurity auskennen, ist unerlässlich für den Schutz Ihres Unternehmens vor Cyberangriffen.

OT-VERANTWORTLICHE

- Informieren Sie Ihre Unternehmensführung weiterhin über die Wichtigkeit, Fragen der OT-Cybersecurity in Angriff zu nehmen. Das mangelnde Verständnis von Führungskräften wird von Cybersecurity-Experten häufig als einer der Hauptgründe für ihre Frustration genannt. Dies gilt allerdings oft für beide Seiten, da sich Führungskräfte immer wieder bei den Cybersecurity-Experten den Cybersecurity-Experten über das mangelnde Verständnis für Geschäftsabläufe beklagen.

Über Bloor

Bloor ist ein unabhängiges Forschungs- und Analystenhaus, das sich nach dem Prinzip „Evolution is Essential" darauf konzentriert, dass die Weiterentwicklung von Unternehmen für deren Geschäftserfolg und Überleben kritisch ist. Seit fast 30 Jahren helfen wir Unternehmen dabei, das Potenzial von Technologien zu erschließen und die für ihre Bedürfnisse optimalen Lösungen zu finden.

Bloor wurde 1989 mit dem Grundsatz gegründet, „Unternehmen dabei zu helfen, die für ihren Erfolg optimalen technologischen Lösungen zu finden". Dazu bieten wir innovative, unabhängige Forschungs- und Beratungsleistungen zum Thema Technologie, die umsetzbare strategische Einblicke liefern. Wir helfen Unternehmen, während ihrer Transformation relevant zu bleiben, neue Ideen in komplexe Geschäftsabläufe einzubringen und Herausforderungen in Gelegenheiten für Wachstum und Profitabilität zu verwandeln.

Im Zeitalter wandlungsfähiger Geschäftsstrukturen ist das Prinzip „Evolution is Essential" bedeutend für den Erfolg. Bloor bringt neues technologisches Denken ein, um Sie bei der Bewältigung komplexer Geschäftssituationen zu unterstützen und Herausforderungen in neue Gelegenheiten für wahres Wachstum, Profitabilität und Einflussnahme zu verwandeln. Wir zeigen Ihnen die Zukunft und helfen Ihnen, Ihr Unternehmen darauf vorzubereiten.

www.bloorresearch.com

Über TÜV Rheinland

Geschäftsbereich Digitale Transformation und Cybersecurity
Seit mehr als 20 Jahren ist es bei TÜV Rheinland die Mission, unsere Kunden bei der sicheren Nutzung von Technologien zu unterstützen. Dazu kombinieren wir unser Fachwissen in den Bereichen digitale Transformation und Cybersecurity mit unserem starken Branchen-Know-how.

Das Dienstleistungsportfolio unserer erfahrenen Berater umfasst innovative Lösungen für die digitale Transformation im Bereich intelligenter Daten, kritischer Infrastrukturen und vernetzter Lösungen. Unser Ansatz für Cybersecurity-Lösungen zielt auf eine einzigartige Kombination von Sicherheit und Datenschutz in einer zunehmend anfälligeren Welt vernetzter Systeme und Geräte ab. Dazu bieten wir pragmatische Lösungen für die Bewältigung von Unternehmensrisiken, die analysebasierte Erkennung von Bedrohungen, automatisierte und manuelle Cybersecurity-Tests, Industrial Security, Datenschutz im Internet der Dinge (IoT) und Sicherung von Cloud-Infrastrukturen an.

Mit einem Team von fast 1.000 Beratern auf der ganzen Welt bieten wir Beratungsdienste, Prüfleistungen und Managed Services für Kunden in allen Branchen sowie in Sicherheitsbehörden, Regierungsorganisationen und öffentlichen Einrichtungen. TÜV Rheinland verfügt über ein weltweites Netzwerk von mehr als 100 modernen Prüflaboren, die unseren Kunden alle notwendigen Prüfungen aus einer Hand bieten – von der Produktsicherheit über Cybersecurity bis hin zum Datenschutz.

www.tuv.com/informationssicherheit

Quellenangaben

Corera, G. (2017, December 30th). If 2017 could be described as 'cyber-geddon,' what will 2018 bring? Retrieved from BBC: https://www.bbc.com/news/technology-42338716

Industrie 4.0. (2018, August 14th). What is Industrie 4.0? Retrieved from Plattform-i40: https://www.plattform-i40.de/I40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html

Intel Corporation. (2018, August 28th). 50 Years of Moore's Law. Retrieved from intel.com: https://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html

Maw, I. (2018, February 15). How to Use the Industrial Internet of Things (IIoT) in Your Factory. Retrieved from Engineering.com: https://www.engineering.com/AdvancedManufacturing/ArticleID/16506/How-to-Use-the-Industrial-Internet-of-Things-IIoT-in-Your-Factory.aspx

National Institute of Standards and Technology. (2018, April 16th). NIST. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

World Economic Forum. (2018, January 24th). To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity. Retrieved from World Economic Forum: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

Zetter, K. (2014, November 3rd). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved from Wired: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Deutschland
otsecurity@tuv.com

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.