IOT & OT CYBERSECURITY REPORT 2024

Anstieg der Cyberangriffe auf die Industrie — für einen stärkeren Schutz sind dringende Maßnahmen erforderlich.

ONEKEY

CYBERSECURITY REPORT

ZUSAMMENFASSUNG

IoT & OT Cybersecurity Report 2024

Lesezeit: ca. 15 min.

Industrielle Steuerungssysteme, bekannt als Operational Technology (OT), bilden zusammen mit dem Internet der Dinge (IoT) und dem industriellen IoT (IIoT) das digitale Rückgrat der Industrie 4.0. Die heutigen Produktions-, Logistik- und Betriebsprozesse sind ohne OT und IoT kaum vorstellbar. Vernetzte Geräte, Maschinen und Systeme, die kontinuierlich Daten austauschen, sind das Herzstück der modernen Industrie.

Diese zunehmende Konnektivität und Digitalisierung bringt jedoch auch neue Herausforderungen mit sich: Robuste Cybersicherheitsmaßnahmen sind unerlässlich, da IoT-, IIoT- und OT-Systeme trotz anfälliger Software häufig hohe Sicherheitsanforderungen erfüllen müssen. Im Jahr 2024 befragte das Cybersicherheitsunternehmen ONEKEY über 300 IT-Entscheidungsträger und Führungskräfte auf C-Ebene zu ihren Perspektiven und Strategien im Bereich Cybersicherheit. Die Ergebnisse dieser umfassenden Umfrage werden im OT & IoT Cybersecurity Report 2024 vorgestellt.

Wachsendes Bewusstsein für Cyberbedrohungen: Fast 75% der Unternehmen erkennen, dass Hacker zunehmend industrielle Steuerungssysteme und IoT-Geräte ins Visier nehmen.

Ungenügende Schutzmaßnahmen: Vielen Unternehmen fehlt es an ausreichender Abwehr gegen Cyberangriffe, und es bestehen Lücken in der realistischen Risikobewertung, effektiven Präventionsstrategien und umsetzbaren Reaktionsmöglichkeiten.

Wissenslücken im Bereich Compliance: Zahlreiche Unternehmen sind unzureichend über die relevanten Compliance-Anforderungen informiert, und fast die Hälfte kennt die technischen Cybersicherheitsstandards nicht.

Veraltete Firmware als Sicherheitslücke: Veraltete Firmware in Geräten und Maschinen wird zunehmend von Hackern als Einstiegspunkt ausgenutzt. Angriffe auf ungeschützte Firmware können verheerende Folgen haben und möglicherweise ganze Produktionschargen zum Stillstand bringen.

Fehlende Software-Stückliste (SBOM): Über der Hälfte der Unternehmen fehlt es an vollständigen SBOMs, obwohl diese für eine effektive Cybersicherheit unerlässlich sind.

Budgetbeschränkungen: 60% der Unternehmen bewerten ihr Budget für Cybersicherheit als unzureichend oder unsicher, und nur 34% halten es für „ausreichend“ oder „erheblich“.

Unzureichende Cybersicherheitsprozesse: Nur etwa ein Viertel der Unternehmen bewertet den Reifegrad ihrer Cybersicherheitsprozesse als ausreichend, und vielen fehlen Maßnahmen, um die Sicherheitspraktiken zu verbessern und die Compliance-Anforderungen zu erfüllen.

UNTERSCHÄTZTES RISIKO: OT UND IOT

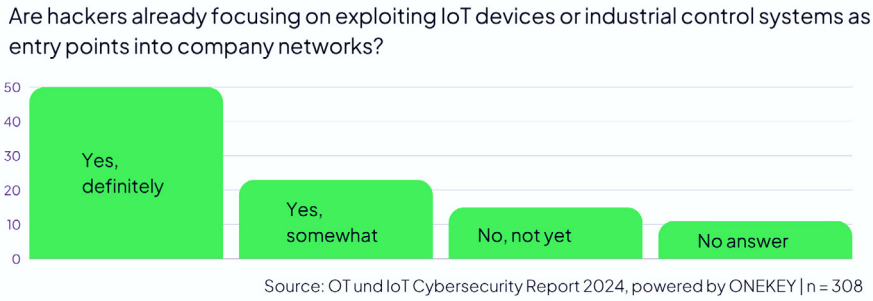
Die Studie zeigt deutlich, dass Cybersicherheit in OT und IoT erhebliche Risiken birgt, doch viele Unternehmen sind immer noch nicht ausreichend vorbereitet. Mehr als die Hälfte der Befragten (52%) hat bereits Cyberangriffe durch OT- oder IoT-Geräte erlebt, und ebenso viele vermuten, dass Cyberkriminelle gezielt auf diese Geräte als Einstiegspunkte abzielen. Dennoch wird OT- und IoT-Cybersicherheit oft als weniger kritisch angesehen.

Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

„Angesichts der Tatsache, dass jeden Monat über 2.000 neue Software-Sicherheitslücken identifiziert werden, fragen Unternehmen, die ihre Software nicht auf dem neuesten Stand halten, nicht, ob sie Ziel von Cyberangriffen werden, sondern wann — und wie schwerwiegend die Folgen sein werden.“ – Jan Wendenburg, Geschäftsführer ONEKEY.

Stattdessen konzentrieren sich viele Unternehmen mehr auf den Schutz von Zahlungs- und Finanzsystemen (42%), Unternehmensnetzwerken und Rechenzentren (39%) sowie Kundendaten (36%). E-Mail, Cloud-Dienste und Apps werden ebenfalls als größere Bedrohungen wahrgenommen, während die Risiken für OT (Operational Technology) und IoT (Internet der Dinge) oft unterschätzt werden.

Mit der fortschreitenden Digitalisierung auf Produktions- und Logistikebene in der deutschen Industrie tauchen immer mehr Sicherheitslücken auf — und das schafft neue Angriffspunkte für Cyberkriminelle.



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

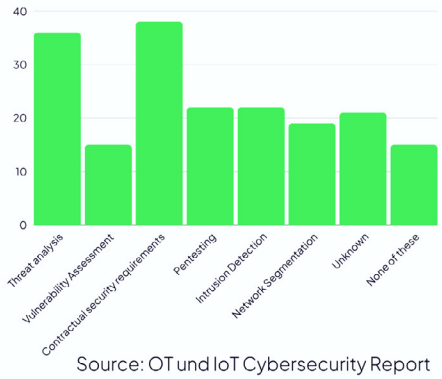
CYBER-RESILIENZ: EINE REALISTISCHE SELBSTEINSCHÄTZUNG

Mehr als ein Viertel (26%) der Unternehmen hält ihren Reifegrad im Bereich Cybersicherheit in der Produkt- und Projektentwicklung dank eines definierten und aktiven Sicherheitsprozesses für „ausreichend“. Weitere 12% verfügen über Sicherheitsprozesse, halten ihre Kontrollmaßnahmen jedoch für unzureichend. Unterdessen geben 9% der Unternehmen an, überhaupt keine derartigen Prozesse zu haben.

Unternehmen konzentrieren sich auf eine Vielzahl von Maßnahmen, um ihre Cyber-Resilienz zu verbessern: 36% führen Bedrohungsanalysen durch, 23% nutzen Penetrationstests, 22% verlassen sich auf Systeme zur Erkennung von Eindringlingen und 15% konzentrieren sich auf Schwachstellenanalysen. 19% der Unternehmen setzen eine Netzwerksegmentierung ein, um die Auswirkungen von Angriffen zu begrenzen. Insbesondere betrachten 38% der Unternehmen die Sicherheitsgarantien ihrer IT-Dienstleister und Lieferanten als die „wichtigste“ Maßnahme.

Was die Mittelzuweisung anbelangt, so hält ein Drittel der Befragten die Mittel zur Abwehr von Cyberangriffen für „begrenzt“ und sieht Verbesserungspotenzial. In 27% der Unternehmen ist die Haushaltslage für Cybersicherheit unklar. Nur 34% verfügen über ein „angemessenes“ oder „erhebliches“ Budget, um ihre Cyber-Resilienz zu stärken.

What measures does your organization take to ensure the security of the IoT infrastructure? (Multiple answers possible)



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

„Viele Unternehmen scheinen der Cybersicherheit erst dann Priorität einzuräumen, wenn bereits ein Vorfall stattgefunden hat.“ – Jan Wendenburg, Geschäftsführer ONEKEY.

Weniger als ein Drittel (32%) der in der Studie befragten Unternehmen haben Verfahren eingeführt, um aus Sicherheitsvorfällen zu lernen und notwendige Verbesserungen vorzunehmen. Angesichts der anhaltenden Bedrohungslandschaft sollten vordefinierte Geschäftsprozesse, die den Umgang mit Cyberangriffen sowohl während als auch nach einem Vorfall regeln, Teil des Sicherheitsrepertoires jedes Unternehmens sein.

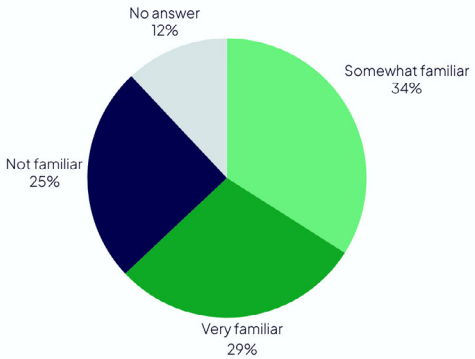
Positiv zu vermerken ist, dass gut ein Drittel (34%) der Unternehmen einen Sicherheitsvorfall nach einem Cyberangriff gründlich analysiert und bewertet, um daraus konkrete Verbesserungsmaßnahmen abzuleiten.

MANGELNDE KENNTNIS DER GESETZLICHEN CYBERSICHERHEITS-ANFORDERUNGEN

Ab 2026/2027 verpflichtet der EU Cyber Resilience Act (CRA) alle Hersteller von Geräten, Maschinen und Anlagen, die Produkte in der EU verkaufen, zur Erfüllung verstärkter Cybersicherheitsanforderungen. Die Studie zeigt jedoch, dass viele Unternehmen darauf noch nicht ausreichend vorbereitet sind. Nur 28% der befragten Unternehmen haben spezifische Compliance-Vorschriften für die Sicherheit von industriellen Steuerungssystemen oder IIoT-Geräten. Für ein Drittel (34%) sind OT- oder IoT-Sicherheitsvorschriften Teil der allgemeinen Cybersicherheitsrichtlinien des Unternehmens, werden aber nicht speziell behandelt. Beunruhigenderweise haben 19% der Unternehmen keine besonderen Vorkehrungen in diesem Bereich getroffen. Ein Fünftel der Befragten war entweder nicht in der Lage oder nicht bereit, Informationen bereitzustellen, was auf erhebliche Unsicherheiten und ein hohes Maß an Unbekannten hindeutet.

Weniger als ein Drittel (29%) der Befragten gibt an, mit den für ihre Branche relevanten Vorschriften und Cybersicherheitsstandards vertraut zu sein. Ungefähr ein Drittel (34%) hat begrenzte Kenntnisse, während 25% überhaupt keine Kenntnisse haben. Angesichts der typischen Entwicklungszeiten von zwei bis drei Jahren laufen Unternehmen, die nicht rechtzeitig handeln, Gefahr, ihre Produkte ab 2027 nicht mehr in der EU verkaufen zu können, wenn sie die Anforderungen bis dahin nicht erfüllt haben.

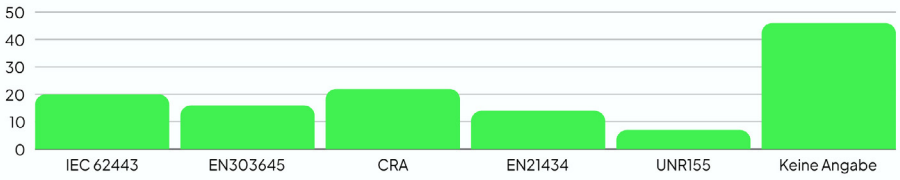
Are you familiar with the cybersecurity regulations relevant to your industry?



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

Darüber hinaus konnten 46% der befragten Unternehmen nicht angeben, welche Cybersicherheitsstandards für ihre Produktentwicklung relevant sind. Die Bedeutung dieser Standards wird oft unterschätzt: Nur 23% halten den EU Cyber Resilience Act (CRA) für relevant. Andere Normen wie IEC62443 (20%), EN 303 645 (16%), EN 21434 (14%) und UNR155 (8%) werden ebenfalls nur von einer Minderheit als wichtig angesehen. Dies unterstreicht die erhebliche Informationslücke in Bezug auf die Einhaltung der Vorschriften.

Which cybersecurity standards are relevant to your organization in product development?

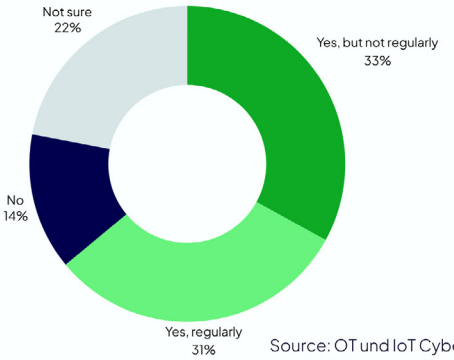


Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

UNZUREICHENDE SICHERHEITSTESTS UND PATCH-MANAGEMENT FÜR IOT-GERÄTE

Bei der Beschaffung von IoT-Geräten führen nur 29% der Industrieunternehmen gründliche Sicherheitstests durch. 30% beschränken sich auf oberflächliche Tests oder Stichproben, während 15% überhaupt keine Sicherheitskontrollen durchführen. Die wichtigsten Unternehmen haben zu diesem Thema keine Informationen zur Verfügung gestellt. Ein ähnliches Muster zeigt sich bei der Analyse der Gerätefirmware: Weniger als ein Drittel (31%) der Unternehmen führen regelmäßige Sicherheitstests durch, um Sicherheitslücken in der eingebetteten Software zu identifizieren. 47% testen die Firmware nur gelegentlich oder gar nicht, und 22% gaben keine Informationen zu diesem Thema an.

Is device firmware analysis — checking the IoT device's internal software for vulnerabilities — practiced in your organization?



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

„Jeder, der die Installation eines Patches verzögert, setzt sich einem erheblichen Risiko aus, da Cyberkriminelle das Zeitfenster zwischen Entdeckung und Behebung gezielt ausnutzen." – Jan Wendenburg, Geschäftsführer ONEKEY.

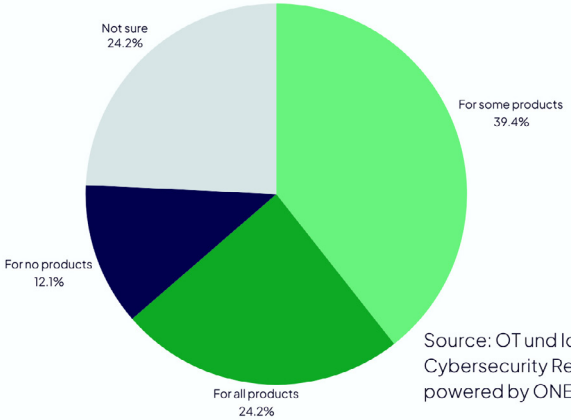
In Bezug auf Softwareupdates aktualisieren 33% der Unternehmen ihre Geräte sofort, nachdem ein Patch verfügbar ist. Im Gegensatz dazu warten 31% bis zur nächsten geplanten Veröffentlichung, während 10% nach der Auslieferung keine weiteren Updates bereitstellen. Weitere 26% der Befragten sind sich bezüglich der Aktualisierungsrichtlinien ihrer Geräte nicht sicher.

Auf die Frage, ob die Cybersicherheit bereits eingesetzter Geräte überprüft wird, antworten 28% der Unternehmen, dass sie dies automatisch tun. 30% führen gelegentlich manuelle Überprüfungen durch, während 17% keine weiteren Sicherheitsbewertungen durchführen. Das Warten auf geplante Updates birgt jedoch erhebliche Risiken, da Cyberkriminelle häufig das Zeitfenster zwischen Entdeckung und Behebung ausnutzen.

SBOM: IMPLEMENTIERUNG FEHLT NOCH

Laut der Umfrage verfügen weniger als ein Viertel (24%) der Industrieunternehmen über eine vollständige Software-Bill Of Materials (SBOM). Während Software für Computer und Netzwerke in der Regel dokumentiert ist, fehlt vielen Unternehmen ein Überblick über die Software in Geräten, Maschinen und Anlagen. Dies ist problematisch, da veraltete Software in Steuerungssystemen ein häufiger Einstiegspunkt für Hacker ist. Typische Beispiele hierfür sind Fertigungsroboter, CNC-Maschinen und Gebäudeautomationssysteme. Diese Systeme sind mit dem Unternehmensnetzwerk verbunden, wodurch eine erhebliche Angriffsfläche entsteht. Die Mehrheit der Unternehmen hat jedoch entweder keine oder nur eine unvollständige SBOM.

If you use products with digital components (chips, hardware with embedded firmware, etc.) in your organization — do you have a Software Bill of Materials for them?



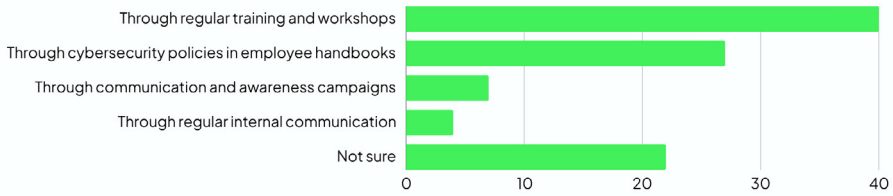
Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

SCHULUNGEN UND AUDITS: UNVERZICHTBAR FÜR EIN STARKES BEWUSSTSEIN FÜR CYBERSICHERHEIT

Ein positiver Trend zeichnet sich ab, aber es besteht noch erhebliches Verbesserungspotenzial. 40% der Industrieunternehmen bieten ihren Mitarbeitern regelmäßige Schulungen und Workshops zur Cybersicherheit an. 27% haben Cybersicherheitsregeln in ihre Mitarbeiterhandbücher und Unternehmensrichtlinien integriert.

Darüber hinaus führen 62% der befragten Unternehmen regelmäßige Cybersicherheitsaudits durch. 24% verlassen sich auf externe Bewertungen, 18% auf interne Audits und 20% verwenden eine Kombination aus beiden Ansätzen. Für mehr als ein Drittel der Unternehmen ist jedoch unklar, ob und in welchem Umfang regelmäßige Cybersicherheitsüberprüfungen durchgeführt werden.

How are employees made aware of their role and responsibility in maintaining cybersecurity?



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

ONEKEY
onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

V20250117DE