# Die Lage der OT-Cybersicherheit 2024/2025

## Metriken und Trends global und lokal




NIS2-COMPLIANCE IN DER OT SICHERSTELLEN

SCHWACHSTELLEN UND SICHERHEITSVORFÄLLE IN DER OT ERKENNEN

FACHKRÄFTEMANGEL IN DER OT-SICHERHEIT ÜBERBRÜCKEN

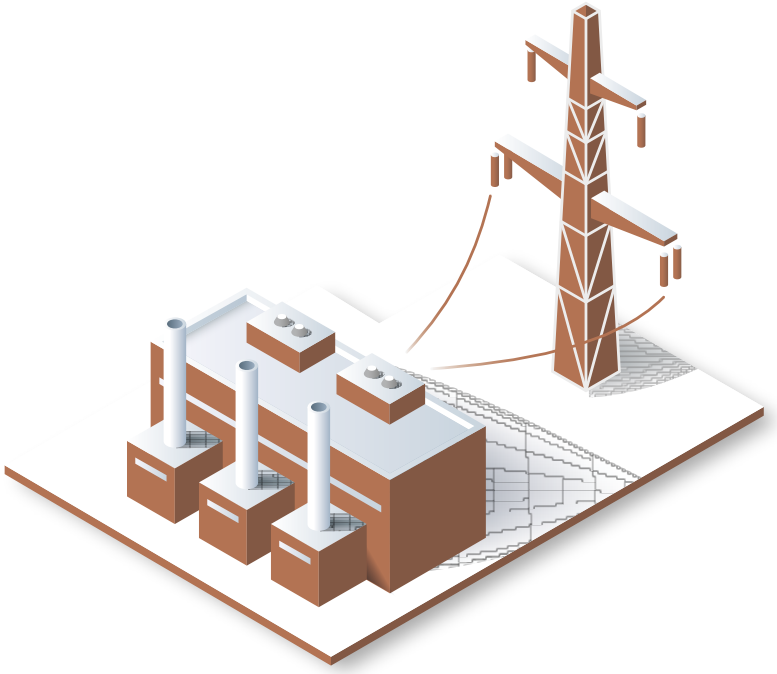
# Einleitung

OT-Cybersicherheit wird nicht erst seit der NIS2 Direktive und den nationalen Umsetzungsgesetzen integraler Bestandteil jeder Cybersicherheitsstrategie. Cybervorfälle, die auch 2024 zu einer Vielzahl von Stillständen in Produktionssystemen und Störungen in Versorgungsinfrastrukturen geführt habe, verdeutlichen seit Jahren, wie eng IT und OT, digitale Welt und physische Prozesse längst verbunden sind. Mit dieser Vernetzung werden auch Arbeits- und Umweltschutz zu Aspekten der Cybersicherheit eines Unternehmens.

Selbst wenn 2024 nur eine Handvoll Angriffe gezielt auf OT-Netzwerke bekannt geworden sind: die Risikolandschaft entwickelt sich rasant weiter – von Living-off-the-Land-Methoden bis zum Wachstum von Infostealern und Access Brokern, die gezielt Daten für eine spätere Netzwerkpenetration sammeln. Auch 2024 war ein Rekordjahr für Schwachstellen industrieller Komponenten und Systeme. Geopolitische Konflikte und Cyberkriminalität gehen zusehends enger Hand in Hand. Prepositioning-Aktivitäten staatlicher Advanced Persistent Threats waren und sind nur ein Hinweis darauf, wie gezielt und langfristig die Akteure beim Erreichen ihrer Ziele vorgehen. Die steigenden Angriffszahlen auf die IT sowie die zunehmende Vernetzung zwischen IT und OT erhöhen weiter die Risiken in der OT.

Auch die Ergebnisse aus Rhebo Industrial Security Assessments, während derer OT-Netzwerke auf bestehende Sicherheitsrisiken untersucht werden, verdeutlichen die offenen Flanken industrieller Infrastruktur. Ob Legacy-Protokolle, veraltete und lückenhafte Authentifizierungsmethoden oder OT-Komponenten, die per Werkeinstellung automatisch und bislang unbemerkt Verbindungen ins Internet aufbauen: die OT bietet mehr als einen Angriffsvektor. Dass bisher weltweit nur wenige größeren Vorfälle direkt in der OT bekannt geworden sind, kann nur damit begründet werden, dass die klassischen Angriffsvektoren (in die IT) bislang noch immer lukrativer und einfacher sind.

Dieser Bericht fasst aus verschiedenen offiziellen Quellen die Entwicklungen und Informationen zur Cybersicherheit in industriell geprägten Unternehmen zusammen. Die Datenlage ist bei weitem nicht so konsistent, wie einzelne Berichte suggerieren. So sind viele Daten aufgrund langsamer Meldungs- und Auswertungsprozesse für 2024 unvollständig und werden sich in den nächsten Monaten weiter verändern. Der Bericht verfolgt die Metriken und Trends von der globalen über die europäische bis zur deutschen Perspektive und schließt mit den spezifischen Beobachtungen aus dem Arbeitsumfeld von Rhebo.



## Inhalte des Ebooks

# **Die globale Perspektive** auf OT-Sicherheit

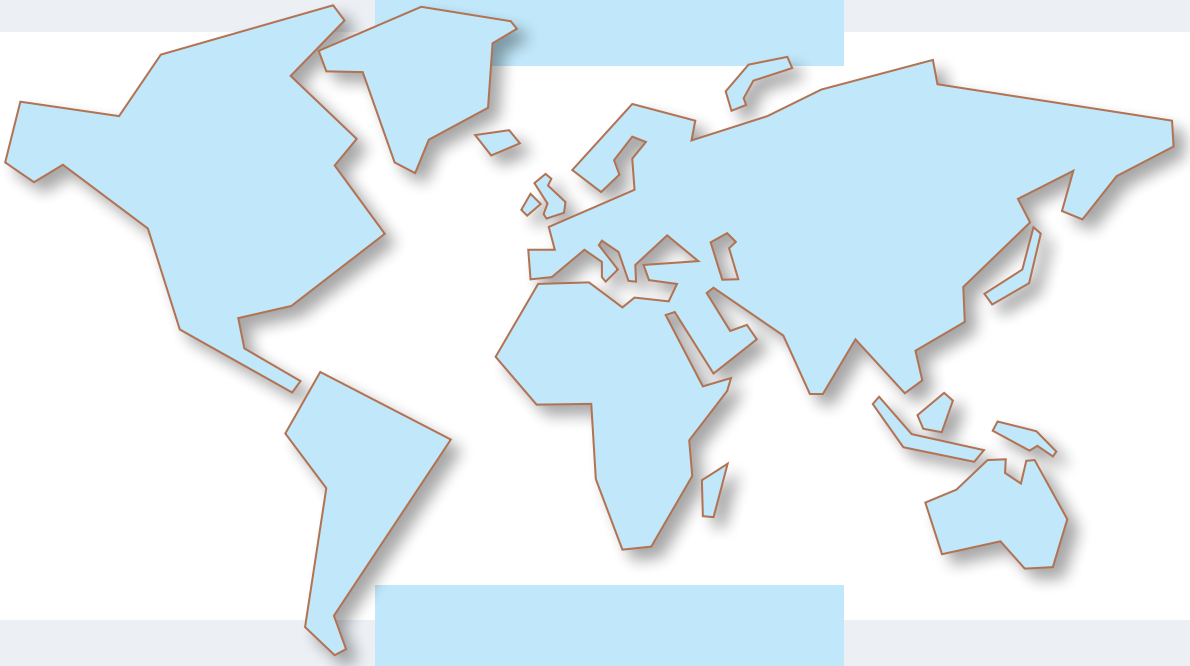
## Metriken

**76**

**Berichte**
über OT-relevante Cyberangriffe

Berichte über Cyberangriffe, welche die OT beeinträchtigten, sind **relativ uneinheitlich** und abhängig davon, wo die Analyst:innen die Grenzen ziehen. Öffentlichen Berichten zufolge hatten im Jahr 2024 nur 76 der gemeldeten Cyberangriffe Auswirkungen auf physische Prozesse (ein Anstieg um 300 % seit 2020), allerdings waren aufgrund der Vernetzung dabei etwa **1.076 Industriestandorte betroffen** (ein Anstieg um fast 1.000 % seit 2020).[1]

Dessen ungeachtet belegen weltweite Umfragen von CISOs und deren Cybersicherheitsteams, dass 50 bis 70 % der Cyberangriffe auf Industrieunternehmen **durch »spill-over« auch Auswirkungen auf die OT hatten.** Davon beeinträchtigten 20–38 % den **Arbeitsschutz und die Anlagenverfügbarkeit,** wodurch sich der Scope von Cybersicherheit in die physische Welt erweitert.[2, 3]

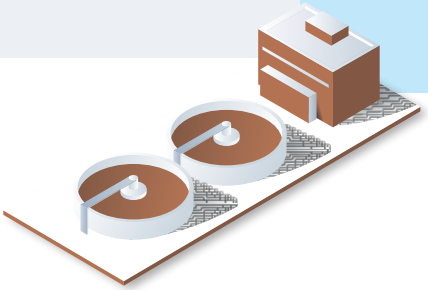


**57**

Prozent
**kritische Infrastruktur**
betroffen

Unter den Opfern von Cyberangriffen auf Unternehmen mit Meldepflicht nimmt die kritische Infrastruktur eine zentrale Rolle ein. Demnach betrafen **2024** von 732 ausgewerteten Angriffen insgesamt **418 kritische Infrastruktur Unternehmen**[4] (Stand 10.03.2025). Aufgrund der verzögerten Meldungen und Auswertungen werden regelmäßig weitere zu den Statistiken hinzugefügt.

Da in nur verhältnismäßig wenigen Ländern strikte Berichtspflichten und öffentliche Bekanntmachungen zu Cybervorfällen existieren, dürfte die **Dunkelziffer** der gemeldeten Fälle zudem **um einiges höher** liegen. Am 1. April 2025 hat die Schweiz als letztes Land die Meldepflicht für Cybervorfälle eingeführt. Durch solche nationalen Entscheidungen könnten die Daten zu Vorfällen in Zukunft zuverlässiger werden.[5]

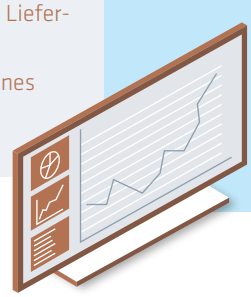


Insgesamt bewertet die globale Wirtschaft die Cyberrisikolandschaft zunehmend komplexer. **45 %** der durch das World Economic Forum befragten **CISOs befürchten am meisten eine Störung des Betriebs.** Die Gründe sind vielfältig:

- Geopolitische Krisen machen Angriffe als Teil der hybriden Kriegsführung immer wahrscheinlicher.
- Komplexe, häufig intransparente Lieferketten erhöhen den Eintrag von Schwachstellen und das Risiko eines Supply Chain Comprimise.

# 45

Prozent befürchten
**Betriebsstörung**



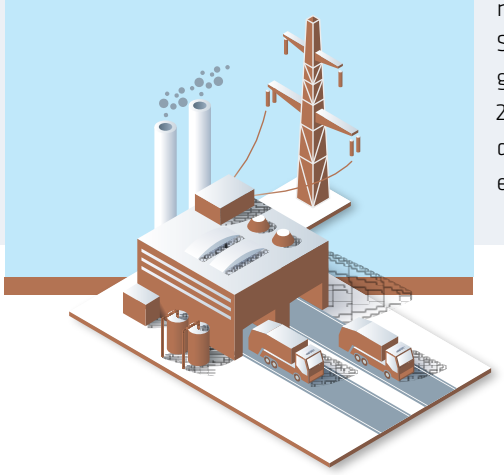
- Die schnelle (häufig ungeprüfte) Anwendung neuer Technologien erhöht das Risiko von Sicherheitslücken.
- Im Bereich der OT/IoT erweitert sich die CIA-Triade (Confidentiality, Integrity und Availability) um die Sicherheit von Mensch und Umwelt.
- Der Fachkräftemangel im Bereich der Cybersicherheit steigt um weitere 8%.[6]

Diese Gründe werden auch in den kommenden Jahren nicht abnehmen – im Gegenteil.

OT-Komponenten und –Systeme bleiben weiterhin mehrheitlich insecure-by-design. Insbesondere ältere Versionen, die in der OT nicht selten Lebenszyklen von 10 – 20 Jahren aufweisen, sind **von Schwachstellen und bleibenden Sicherheitslücken betroffen.** Die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA) veröffentlichte 2024 insgesamt 432 ICS Advisories[7] über bekannt gewordene Schwachstellen und Gefährdungen, ein **Anstieg von 8,8 Prozent** im Vergleich zu 2023.

# 432

**ICS Advisories**



Der Großteil der **Cyberangriffe,** die Industrieumgebungen beeinträchtigten erfolgten jedoch nach wie vor **über die IT,** für deren Komponenten und Systeme im Zeitraum Juli 2023 bis Juni 2024 **über 33.000 Schwachstellen** gemeldet wurden – **36 % mehr** als im Vorjahreszeitraum.[8] Von diesen waren 76 % über das Netzwerk ausnutzbar. Zunehmend werden aber auch Fernzugänge und Supply Chain Compromise als Angriffsvektor genutzt (Abbildung 1).[9] Zusätzlich wurden 2024 mit FrostyGoop, IOControl und Fuxnet drei neue Schadsoftware-Kits bekannt, die explizit OT-Komponenten ausnutzten.

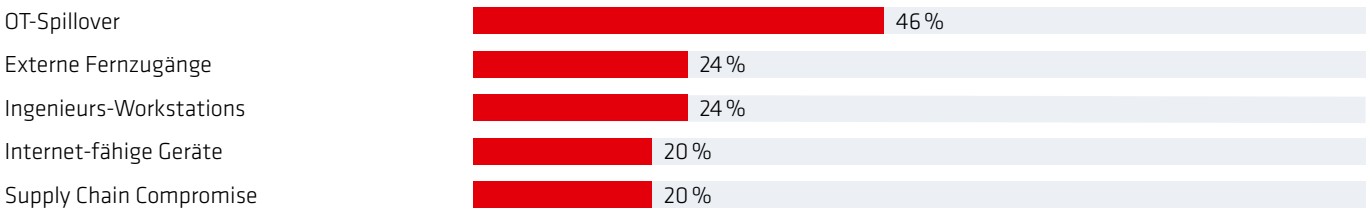



**Abbildung 1** Top 5 der initialen Angriffsvektoren auf Industrieunternehmen

## Trends Cyberangriffe

Die Tactics, Techniques & Procedures (TTPs) der Angreifenden werden ausgefeilter. Zugleich ist bereits seit einigen Jahren die rote Linie der kritischen Infrastrukturen bei Cyberkriminellen und staatlich gestützten Angreifenden gefallen. So wurde im Oktober 2024 American Water Opfer eines Cyberangriffs. Das größte US-amerikanische Wasser- und Abwasserunternehmen versorgt 14 Millionen US-Bürger:innen und 18 militärische Einrichtungen[10]. Der Angriff beeinträchtigte nach ersten Berichten zwar nur das Abrechnungswesen, verdeutlicht jedoch den Trend, dass kritische Infrastrukturunternehmen nicht mehr verschont bleiben.

CISA und eine Reihe Geheimdienste warnten im Februar 2024 vor der Gefahr der Präpositionierung. Demnach wären einzelne Advanced Persistence Threats (ATPs) nicht mehr auf eine sofortige Störung aus, sondern auf eine langfristige, strategische Positionierung (prepositioning) und Verfestigung (evasion, persistence) an neuralgischen Punkten in den jeweiligen Netzwerken. Ziel sei die Fähigkeit, im Falle eines vermutlich geopolitischen Konflikts sofort zuschlagen zu können[11].

In diesem Rahmen werden zunehmend TTPs eingesetzt, die eine Detektion durch konventionelle Perimetersicherung (z. B. Firewalls, Authentifizierung) verschleiern. Insbesondere so genannte Living-Off-The-Land-Techniken (LOTL) finden verstärkt Anwendung, bei denen die gegebene Infrastruktur ausgenutzt wird, ohne zusätzliche Payloads und Malware einzubringen[12]. Zusätzlich wurden Fälle aufgedeckt, bei denen nordkoreanische Akteure unter falschen Identitäten und Lokalisierungen als Remote-IT-Worker Unternehmen infiltrierten, Daten stahlen und die Unternehmen erpressten[13].

Als Angriffsvektoren rücken zunehmend Edge Networking Devices und Fernzugangstechnologien in den Fokus – 2024 u.a. Komponenten von Juniper, Sophos, Ivanti, Cisco, PaloAlto, Fortinet, FortiGate und Citrix[14]. In vielen Fällen wurden gezielt Zero-Day-Schwachstellen ausgenutzt.[15]

Dessen ungeachtet wurden 2024 nur wenige Cyberangriffe bekannt, die offensichtlich direkt auf OT-Infrastrukturen zielten. In der Regel war die Unternehmens-IT entweder Hauptopfer oder Ausgangspunkt für Störungen in der OT (spillover). Jedoch muss berücksichtigt werden, dass die fehlenden Zahlen auch aufgrund verschiedener Faktoren zustande kommen können, u.a.:

- falsche Attribution von Angriffen,
- fehlende Sichtbarkeit in der OT und damit fehlende Detektion von Angriffen auf die OT (siehe Interview S. 12)
- lückenhafte Meldung von Vorfällen aufgrund fehlender Infrastruktur und Prozesse sowie aufgrund von Sicherheitsbedenken bei einer Bekanntmachung.

## Trends OT-Cybersicherheit

Auf der abwehrenden Seite der OT-Sicherheit zeigen sich zwei gegenläufige Trends. Zum einen werden auch die OT-Netze immer offener gestaltet. IT/OT-Konvergenz, Cloud-Anbindung, Fernzugriff und Fernsteuerung sowie Integration von Künstlicher Intelligenz verringern immer stärker die Autonomie der OT von der Außenwelt und der Unternehmens-IT.

Zum anderen kämpft die OT-Sicherheit noch immer mit inhärenten Limitierungen wie Legacy-Systemen, High-Privilege-Zugang von Dienstleistern und Herstellern[16], fehlender Segmentierung und Sichtbarkeit. Gleichzeitig etablieren sich netzwerkbasierte Angriffserkennungssysteme (NIDS für Network Intrusion Detection Sytem) immer stärker als Werkzeug der OT-Sicherheit[17]. So hat die North American Electric Reliability Corporation (NERC), die verbindliche Standards für u.a. den Energiesektor erarbeitet, 2024 mit dem CIP-015 einen Standard definiert, der explizit die Anforderungen an ein Network Security Monitoring definiert[18]. Der Standard wird vermutlich im Laufe dieses Jahres verbindlich werden.

*»Die Diskussion der rein kommerziellen Seite wird der OT nicht ganz gerecht, denn manchmal investiert man in den Arbeitsschutz und in den Schutz vor Dingen, die nicht passieren sollen. Das Verständnis für die Folgen von Sicherheitsverletzungen ist etwas anders. OT-CISOs, oder deren Organisationen, werden dabei helfen, diese Botschaft an die Unternehmen zu übermitteln«.*

Mohammed Adel Saad | Chief IT/OT Cybersecurity Advisor, innovAKT
im Rhebo-Podcast OT Security Made Simple:
»Was die NIS 2 Direktive für Industrieunternehmen bedeutet.«[19]

# **Die europäische Perspektive** auf OT-Cybersicherheit

## Metriken

Die Daten für Cybervorfälle sind in der EU weitaus weniger aussagekräftig, da es bei der Meldung auf EU-Ebene zu **starken Verzögerungen** kommt. Während für 2023 der ENISA über 1.200 Vorfälle von den nationalen CSIRTs gemeldet wurden, lagen Stand 11. Februar 2025 nur 230 Meldungen für das Jahr 2024 vor. Diese Zahl wuchs bis zum 11. März 2025 bereits auf 575 Meldungen an – Tendenz: steigend. Davon wurden bislang **34 % bösartigen Akteuren zugeordnet.**[20]

**3.000**

**Angriffe**
auf industrielle Unternehmen

Dagegen verzeichnete die Agentur der Europäischen Union für Cybersicherheit (ENISA) für den Zeitraum **Juli 2023 bis Juni 2024** insgesamt **9.800 Cybervorfälle in der EU.** Rund ein Drittel davon trafen industriell geprägte Unternehmen (Abbildung 2). **Die Top 5 der Gefährdungen** bildeten demnach DDoS, Ransomware, Datendiebstahl, Malware und Social Engineering.[21]
In Großbritannien nahmen die dem National Cyber Security Centre (NCSC) gemeldeten Vorfälle bereits **bis Oktober 2024 um 50 % im Vergleich zum Vorjahr zu.**[22]

Auch in der EU bleibt der Fachkräftemangel eine der größten Herausforderungen für die Unternehmen. **Fast zwei Drittel** der Unternehmen gaben bei der Besetzung von Stellen in der Cybersicherheit **Schwierigkeiten an, qualifiziertes Personal zu finden.**

**70**

Prozent
kämpfen mit
**Fachkräftemangel**

76 % der in der Cybersicherheit Angestellten hätten zudem keine formelle Qualifikation oder Zertifizierung in dem Bereich. Die **Skills Gap kletterte** deshalb 2024 von Platz 8 **auf Platz 2 der größten Cyberrisiken**.[23]

## Trends Cyberangriffe

Die ENISA bewertet das Cyberrisiko für Europa generell als »substantial«. Das bedeutet, dass eine hohe Wahrscheinlichkeit für Angriffe vorliegt und die Störung essenzieller und wichtiger Entitäten als realistisch angesehen wird.[24] Dabei verzeichnet die ENISA – vergleichbar mit globalen Beobachtungen – eine Weiterentwicklung der TTPs. Angreifende würden demnach immer stärker auf verschleierte Angriffe setzen, die durch Firewalls und Virusscanner übersehen werden. Dazu gehören neben LOTL-Techniken, fileless malware und Zero-Day-Exploits auch Supply Chain Compromise (insbesondere Open-Source Libraries) und gestohlene Zugangsdaten.[25] Information Stealer Software und Access Broker nahmen in dem Berichtszeitraum weiter zu.[26] Die ENISA schätzt Lieferkettenangriffe in den nächsten Jahren aufgrund von (häufig intransparenten) Softwareabhängigkeiten als größtes Cyberrisiko ein.[27]

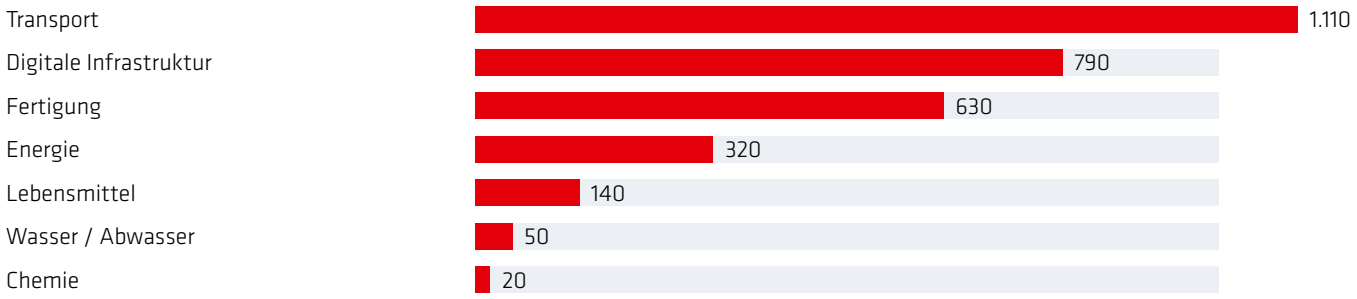



**Abbildung 2** Verteilung der von Cyberangriffen betroffenen Sektoren in der EU 2023/2024

## Trends OT-Cybersichersicherheit

Auf Seite der Cybersicherheit war 2024 ein wichtiges Jahr für die EU. Nicht nur wurde – mit einigen Ausnahmen, u.a. Deutschland – die NIS2-Direktive in nationales Recht umgesetzt und damit über 400.000 Unternehmen EU-weit zu ganzheitlicher Cybersicherheit verpflichtet. Mit dem Cyber Resilience Act wird zudem für alle Anbieter von Produkten mit digitalen Elementen integrale Cybersicherheit zur Pflicht. In der Praxis haben die betroffenen Unternehmen (inklusive kritischer Infrastruktur) dagegen teilweise noch einen weiten Weg vor sich. Sowohl der Fachkräftemangel als auch mangelnde Bugdetierung und Priorisierung für Cybersicherheit – vor allem in der Supply Chain Bewertung – erschweren die Sicherstellung der Cyberresilienz in vielen Unternehmen.[28]

*»Mit den ganzen EU-Richtlinien zu Resilienz und Sicherheit kommt auf die Unternehmen natürlich ein riesiger Bauchladen an Compliance-Themen zu. Viele Unternehmen versuchen, die NIS2-Umsetzung auszusitzen. Wer das macht, spielt Russisches Roulette.«*

Gerald Krebs | TÜV Informationstechnik
im Rhebo-Podcast OT Security Made Simple: »Wer NIS2 aussitzt, spielt Russisches Roulette.«[29]

# **Die deutsche Perspektive** auf OT-Sicherheit

## Metriken

Das BSI beziffert die 2024 **in Deutschland aktiven APTs auf 22.** Diese zielten vorrangig auf Behörden sowie Unternehmen der auswärtigen Angelegenheiten, Verteidigung und öffentlichen Sicherheit und Versorgung.[30] Die **Gesamtzahl der Akteure,** die Deutschland als Ziel haben, **summierte sich jedoch auf 144.** Damit liegt Deutschland im weltweiten Vergleich nach den USA (264 Akteure) auf dem zweiten Platz.[31]

**#2**

der **angegriffenen Länder**

Das BSI erreichten **zwischen Juli 2023 und Juni 2024 insgesamt 726 Meldungen** nach dem IT-Sicherheitsgesetz. Davon fielen 137 auf den Energiesektor, 185 auf den Transport- und Verkehrssektor sowie 22 auf den Wassersektor. Unter den Angriffen fielen mehrere pro-russische Phishing-Kampagnen ins Auge sowie der erfolgreiche Angriff auf PSI, einen deutschen Hersteller für Leitstellen in Energieversorgungssystemen.[32]

Die Anzahl täglich neuer **Schadsoftware-varianten stieg** im Berichtszeitraum des BSI **um 26 %**[33] und erhöhte damit signifikant den Druck auf die Cybersicherheit der Unternehmen und die signaturbasierten Angriffserkennungssysteme.

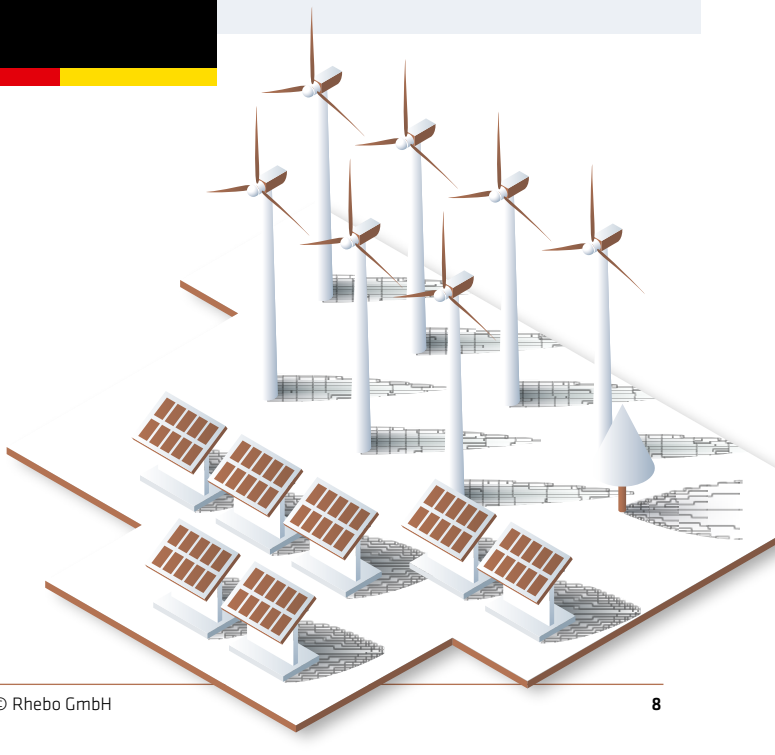
**309**

tausend

**neue Malware-Varianten**

täglich

Der unternehmerische Schaden durch Cyberangriffe belief sich auf fast 179 Milliarden €. Davon entfielen allein **54,5 Milliarden €** (2023: 35 Mrd. €) auf **Störungen von IT- und Produktions-systemen.** Die Anzahl der von Cyberangriffen betroffenen Unternehmen stieg um über 12 %, die Sabotage von IT- und Produktions-systemen um 7%.[34]



## Trends Cyberangriffe

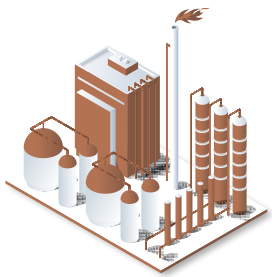
Der deutsche Trend deckt sich weitestgehend mit den europäischen und globalen Entwicklungen. Gezielte Angriffe auf Edge- und Netzwerkgeräte sowie die Zahl der gemeldeten Schwachstellen nahmen demnach auch in Deutschland zu. Das BSI erreichten monatlich 18 Zero-Day-Meldungen in Produkten deutscher Hersteller[35]. Die CISA veröffentlichte 2024 allein für Siemens-Komponenten 150 ICS Advisories (auf Platz 2 lag Rockwell Automation mit 55 Advisories). Grundsätzlich haben diese Zahlen auch eine gute Seite: bekannt gewordene Schwachstellen können auch abgestellt werden.

Im Vergleich zur CISA versuchte das BSI, die Gefahr durch das Prepositioning abzuschwächen[36]. Die Argumentation lässt jedoch offen, ob diese Einschätzung auf nachweisbaren Informationen oder fehlender Sichtbarkeit in vielen (nicht nur OT) Netzwerken basiert. Die Präsidentin des BSI Claudia Plattner zeigte in einem Beitrag zumindest beeindruckende Weitsicht, wenn sie neben Cyber Crime und Cyber Conflict auch das Thema Cyber Dominance (»Einflussnahme durch digitale Produkte, die Herstellern Zugriff auf Informationen und Funktionen ermöglichen«) auf den Tisch bringt und die Übergänge zwischen den drei Kategorien als fließend definiert: »Kriminelle Gruppen agieren heute häufig in staatlichem Auftrag. […] Ist ein Angreifer erst einmal im System, liegen zwischen Spionage und Sabotage leider oft nur zwei Klicks. Noch gefährlicher wird es, wenn Hersteller digitaler Produkte dauerhaften Zugriff auf ihre beim Kunden verbauten Systeme haben, etwa durch regelmäßige Updates.«[37]

## Trends OT-Cybersichersicherheit

Mit der Verschiebung des NIS2-Umsetzungsgesetzes (NIS2UmsuCG) hat die Politik einen wichtigen Meilenstein für die Stärkung der deutsche Cybersicherheit und -resilienz gerissen. Dessen ungeachtet bewertete das BSI das grundlegende Sicherheitslevel Kritischer Infrastrukturen leicht besser als im Vorjahr. 140 von 671 Betreibenden konnten demnach den Reifegrad ihres ISMS verbessern. Dennoch haben in den Sektoren Energie, Wasser und Transport / Verkehr noch immer 69 % nicht alle MUSS-Anforderungen an ein System zur Angriffserkennung (SzA) umgesetzt.[38] Das dürfte vermutlich vor allem an den fehlenden Ressourcen (Knowhow, Zeit, Personal) liegen. Ein weiterer Grund könnte sein, dass noch immer viele Unternehmen davon ausgehen, dass Firewalls und ein Security Information & Event Management (SIEM) System ein performantes, konformes SzA darstellen. Diese Technologien hinterlassen jedoch nicht nur entscheidende Lücken insbesondere in den schützenswerten kritischen Anlagen (der OT). Ihnen fehlen in der Regel auch Funktionalitäten wie Netzwerkmonitoring und Anomalieerkennung.





# **Die Rhebo-Perspektive** auf OT-Sicherheit

Die hier präsentierten Ergebnisse stammen aus Rhebo Industrial Security Assessments, bei denen die Struktur und Kommunikation von OT-Netzen auf bestehende Schwachstellen und laufende Auffälligkeiten untersucht werden (Abbildung 3). Sie verdeutlichen, dass die Herausforderungen in der OT-Sicherheit über die Jahre mehrheitlich gleichgeblieben sind. Es sind vor allem Altlasten, die sichtbar werden und nach und nach beseitigt werden müssen. Das ist nicht verwunderlich, schließlich ist ein Rhebo Industrial Security Assessment für fast alle Betriebe das erste Mal, dass sich mit der eigenen OT-Perspektive der Cybersicherheit und Netzqualität befasst wird.

## Metriken

**100**

Prozent

**unsichere Protokolle**

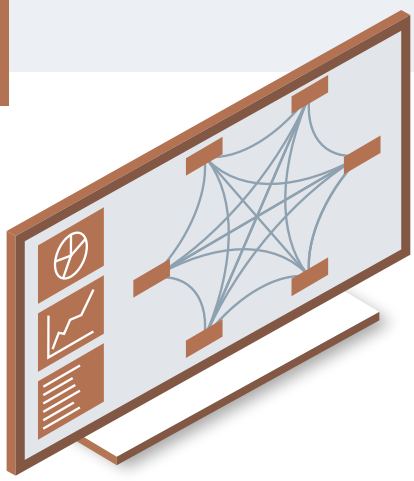
In allen untersuchten OT-Netzwerken fanden sich **protokollbasierte Sicherheitslücken** wie obsolete aber aktive sowie veraltete Protokolltypen. Dazu zählen u.a. Protokolle wie **LLMNR, mDNS oder SSDP.** In der Regel werden diese Protokolle aufgrund ungeprüfter Werkseinstellung von Geräten automatisiert versendet. Sie sind zwar keine akute Gefahr für die Sicherheit. Jedoch können obsolete Protokolle von Angreifenden **als Angriffsvektor verwendet werden.** Darüber hinaus stellen unsichere Protokolltypen wie das veraltete TLS, TFTP oder HTTP weiterhin eine Bedrohung in OT-Netzwerken dar. Diese Protokolle verfügen über keine oder nur **sehr schwache Sicherheitsmechanismen** und können leicht für **Spoofing-Angriffe** ausgenutzt werden.

**100**

Prozent

**unsichere Authentifizierung**

Aufgrund langer Lebenszyklen in den OT-Netzen fanden sich in 100 % aller Assessments **Sicherheitsrisiken bei der Authentifizierung.** In 62,5 % aller untersuchten Netzwerke wurden längst gebrochene Authentifizierungsmethoden aus den 1990er Jahren identifiziert. In allen Netzwerken fanden sich zudem Protokolle, die **keinerlei Authentifizierung** anbieten. Weiterhin kamen in der OT-Kommunikation nach wie vor Protokolltypen zur Anwendung, die **Passwörter in Klartext** versenden und somit gegenüber Spoofing anfällig sind. In einzelnen Fällen wurden Systeme in OT-Netzen identifiziert, die **keinerlei Authentifizierung** anbieten.



Der Anteil **verwundbarer Software, Firmware und Betriebssysteme** ist zwar um 37% auf 63 % gesunken, bleibt aber in Bezug auf die Angriffsfläche aufgrund offener bekannter Schwachstellen eine akute Herausforderung. Verbindungen und Verbindungsversuche von OT-Systemen ins Internet fanden sich in dreiviertel aller Betriebe. In einigen Fällen waren einzelne Systeme sogar **über das Internet sichtbar.**

**63**

Prozent

**verwundbare Systeme**

Bei der Hälfte aller Analysen wurden Geräte in der OT identifiziert, die untypisch oder ungeeignet für industrielle Netzwerke sind. Dazu gehörten u.a. Geräte mit **undurchsichtigen Sicherheitskonzepten** (z. B. chinesische Switches) oder veralteten Protokollen, die ein Einfallstor für **Spionage** bilden können. Aber auch Geräte mit einer mit Ethernet inkompatiblen Kommunikation, die zu **Netzwerkstörungen** führen kann, fanden sich.

**Inkonsistenzen bei der Zeitsynchronisierung** von Systemen sind immer noch **weit verbreitet.** Diese können sich auf OT-Netzwerke in mehrfacher Hinsicht nachteilig auswirken:

- Störung der Authentifizierung,
- erschwerte forensische Analyse von Protokolldateien nach einem Angriff,
- Beeinträchtigung von Echtzeit-Kommunikationsprozessen.

**88**

Prozent

**nicht erreichbare Systeme**

Im Hinblick auf die Stabilität des OT-Netzwerkbetriebs waren **ICMP-Benachrichtigungen über Nichterreichbarkeit** bei 88 % aller Assessments ein häufiges Ereignis. Sie korrelieren oft mit anderen Anomalien wie Übertragungswiederholungen. Diese Warnmeldungen können sowohl von legitimen Wartungsprozessen als auch von Netzwerk- oder Geräteverschleiß oder -ausfällen verursacht werden. Sie geben daher **Aufschluss über die Netzwerkqualität.**

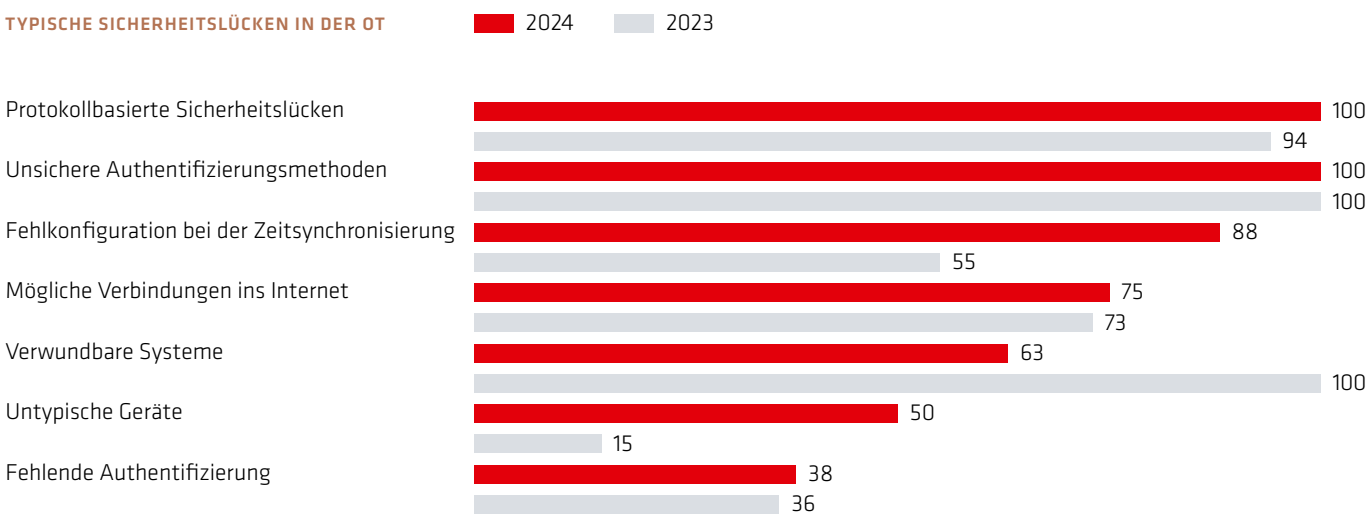



**Abbildung 3** Entwicklung der häufigsten OT-Sicherheitsrisiken zwischen 2023 und 2024

## Trends Cyberangriffe

Die Ergebnisse aus Rhebo Industrial Security Assessments und der Betreuung von Betrieben im Rahmen von Rhebo Managed Protection lassen darauf schließen, dass die Betriebe aktuell nicht mit konkreten Sicherheitsvorfällen in der OT konfrontiert sind. Jedoch bestätigen sie, dass die Betreibenden auf einem äußerst unübersichtlichen – wenn auch vorerst potenziellen – Schlachtfeld stehen, das voller offener Flanken ist.

Neue Geräte, Verbindungen und Kommunikation laufen ohne ein Sicherheitsmonitoring noch immer unter dem Radar der Verantwortlichen. Das ist gerade in industriellen Umgebungen ein besonderes Risiko, in denen mit Systemintegratoren, Systemherstellern und Wartungsdienstleistern eine Vielzahl verschiedener Akteure oftmals tiefreichende Zugriffsprivilegien besitzen.

## Trends OT-Cybersichersicherheit

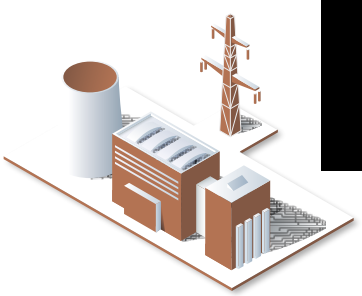
Das Bewusstsein für die Notwendigkeit von OT-Sicherheit ist aufgrund der expandierenden Risikolandschaft in den letzten Jahren gewachsen. Die Intention der Rhebo-Kunden ist eindeutig: Es geht bei der Installation des Systems zur Angriffserkennung nicht nur um gesetzliche Compliance, sondern immer auch um echte Cybersicherheit. OT-Cybersicherheit bleibt dessen ungeachtet in vielen Unternehmen ein neues, mit Unsicherheiten gespicktes Feld. Sicherheitsbeauftragte und Steuerungstechniker:innen stehen in der Regel noch am Anfang ihrer Reise.

Sichtbarkeit, Klarheit und Klärung der bestehenden OT-Infrastruktur und Nutzungsweisen (u.a. des externen Servicepersonals) stehen im Vordergrund. Rhebo-Kunden greifen deshalb regelmäßig auf die Expertise des Rhebo Kundenservices zurück, um gemeldete Anomalien auszuwerten, gegenzuprüfen und Maßnahmen zu beraten. Dieser aktive Wissenstransfer und Ansatz des Training-on-the-Job haben dazu beigetragen, dass das Knowhow zu OT-Sicherheit in den betreuten Betrieben stetig gewachsen ist.

*»Es fehlen die Leute, es fehlt die Technologie und oftmals das Verständnis. Ein Kunde hat zum Beispiel vor ein paar Monaten ein Kraftwerk an die Strombörse gekoppelt. Da wurden ABB und Siemens-Leitsysteme verknüpft. Die Dienstleister, die die Systeme jeweils betreuen, haben das binnen eines Tages in Betrieb genommen. Was mich schon hellhörig werden ließ. Auf meine Frage nach der Dokumentation und den Netzwerkplänen kam die Antwort, dass sie darauf noch warten, aber alles schon laufe. Wir sind dann hingefahren und haben uns das angesehen. Da wurden Netzwerkkabel einfach so gezogen, dass es passt. Die IP-Adressen waren ohne jegliche Dokumentation eingerichtet. Die Kennwörter der Systeme konnten wir relativ schnell herausfinden und dann bis in die SPS runter Werte schreiben. Und das passiert ganz oft.*

*Dass viele Vorfälle nicht gemeldet werden, liegt auch einfach daran, dass sie nicht gesehen werden. Es gibt auch eine deutlich höhere Dunkelziffer an Anlagen, die Vorfälle eigentlich melden sollten, aber weder technisch noch prozessual die Infrastruktur haben, um solche Vorfälle zu melden.«*

Patrick Latus | Unabhängiger Pentester für OT
im Rhebo-Podcast OT Security Made Simple: »Aus dem Tagebuch eines OT-Pentesters.«[39]



# **Bereit für** effektive OT-Sicherheit?

## 1


Der erste einfache Schritt
zu umfassender OT-Sicherheit:
**Rhebo Industrial Security Assessment**

### Cybersicherheit beginnt mit Sichtbarkeit.

Die Rhebo OT-Risikoanalyse und Reifegradbeurteilung des **Rhebo Industrial Security Assessment** liefert ein detailliertes Verständnis der OT-Assets, der Netzwerk- und Kommunikationsstruktur sowie bestehender Sicherheitsrisiken. Unsere Kunden erhalten einen umfassende Übersicht und klare, effektive Handlungsempfehlungen, um die Systemhärtung zu steigern.

### Sie profitieren von

- der Identifikation aller Geräte und Systeme in der OT inklusive ihrer Eigenschaften, Firmware-Versionen, Protokolle und Kommunikationsverbindungen (Asset Discovery & Inventory);
- der detaillierten Analyse bestehender Schwachstellen nach CVE;
- der Identifikation bestehender Gefährdungen, Sicherheitslücken und technischer Fehlerzustände;
- Handlungsempfehlungen mit Abschlussbericht und Workshop.

## 2


Der nahtlose Übergang zu
durchgängiger OT-Sicherheit:
**Rhebo Industrial Protector**

### OT-Sicherheit endet nicht an den Netzwerkgrenzen.

Das OT-Monitoring mit integrierter Angriffserkennung **Rhebo Industrial Protector** schafft dedizierte OT-Sicherheit entsprechend der NIS2. Es erweitert die Absicherung durch Firewalls um eine ganzheitliche Anomalieerkennung innerhalb der OT, ohne kritische industrielle Prozesse zu stören.

### Sie profitieren von

- der Echtzeit-Sichtbarkeit des Kommunikationsverhaltens aller OT- und ICS-Geräte (Protokolle, Verbindungen, Datenraten);
- der Echtzeitmeldung und -lokalisierung von Vorgängen (Anomalien), die auf Cyberattacken, Manipulation und technische Fehlerzustände hinweisen;
- der frühzeitige Identifikation von Angriffen über Backdoors, bislang unbekannte Schwachstellen und Innentätern, die von Firewalls übersehen werden (Defense-in-Depth)

## 3


Wir überwachen, damit Sie sich
um Ihr Kerngeschäft kümmern können:
**Rhebo Managed Protection**

### OT-Sicherheit braucht Ressourcen und Know-How.

Rhebo unterstützt Sie mit **Rhebo Managed Protection** beim Betrieb des OT-Sicherheitsmonitorings mit Anomalieerkennung, insbesondere bei der Auswertung und Reaktion auf Vorfälle sowie der kontinuierlichen Überprüfung und Verbesserung der Abwehrmechanismen.

### Sie profitieren von

- der Unterstützung unserer Expert:innen beim Betrieb des OT-Sicherheitsmonitorings;
- der schnellen forensischen Analyse und Aufklärung von OT-Anomalien;
- der schnellen Handlungsfähigkeit bei Vorfällen;
- regelmäßigen OT-Risikoanalysen für die kontinuierliche Verbesserung des Reifegrads Ihrer Cybersicherheit.

# **Quellen** und Literatur


1 2025 OT Cyber Threat Report, Waterfall, Januar 2025
2 SANS Research: SANS 2024 State of ICS / OT Cybersecurity, Oktober 2024
3 ABi Research: State of OT Security, März 2024
4 European Repository of Cyber Incidents, Januar 2024 – Dezember 2024, *https://eurepoc.eu/table-view* (letzter Zugriff: 11.02.2025)
5 *https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-104400.html* (letzter Zugriff: 17.03.2025)
6 World Economic Forum: Global Cybersecurity Outlook 2025, Januar 2025
7 CISA ICS Advisories 2024 (letzter Zugriff: 11. Februar 2025)
8 ENISA: Threat Landscape 2024, September 2024
9 SANS Research: SANS 2024 State of ICS / OT Cybersecurity, Oktober 2024
10 CNN: *https://edition.cnn.com/2024/10/08/business/american-water-cyberattack-hnk-intl/index.html* Oktober 2024 (letzter Zugriff: 11.02.2024)
11 CISA: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Februar 2024
12 CISA: Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance, Februar 2024
13 Bill Toulas: Undercover North Korean IT workers now steal data, extort employers, BleepingComputer, Oktober 2024
14 Lawrence Abrams: The biggest cybersecurity and cyberattack stories of 2024, BleepingComputer, Januar 2025
15 *https://www.hackmageddon.com/2024/04/22/cves-targeting-remote-access-technologies* (letzter Zugriff: 11.02.2025)
16 ABi Research: State of OT Security, März 2024
17 SANS Research: SANS 2024 State of ICS / OT Cybersecurity, Oktober 2024
18 *https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-015-1.pdf* (letzter Zugriff: 10.02.2025)
19 OT Security Made Simple, Wie übersetzt man IT-Sicherheit in OT-Sicherheit?, Januar 2025, *https://rhebo.com/de/podcasts/wie-ubersetzt-man-it-sicherheit-in-ot-sicherheit*
20 *https://ciras.enisa.europa.eu/* (letzter Zugriff: 11.03.2025)
21 ENISA, Threat Landscape 2024, S.14 – 16, September 2024
22 *https://therecord.media/uk-nationally-significant-cyberattacks-ncsc-horne-warning* (letzter Zugriff: 12.02.2025)
23 ENISA, 2024 Report on the state of cybersecurity in the union, S. 49, Dezember 2024
24 ENISA, 2024 Report on the state of cybersecurity in the union, S. 14, Dezember 2024
25 ENISA, Threat Landscape 2024, S. 58 – 59, September 2024
26 ENISA, Threat Landscape 2024, S. 30, September 2024
27 *https://www.enisa.europa.eu/topics/cyber-threats/foresight* (letzter Zugriff: 12.02.2025)
28 ENISA, 2024 Report on the state of cybersecurity in the union, S. 49 – 54, Dezember 2024
29 OT Security Made Simple, Wer NIS2 aussitzt, spielt Russisches Roulette, Dezember 2024, *https://rhebo.com/de/podcasts/er-nis2-aussitzt-spielt-russisches-roulette*
30 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 9, 2024
31 Forescout, 2024 Threat Roundup, S. 22, 2024
32 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 63 und 66, 2024
33 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 15, 2024
34 Bitkom, Wirtschaftsschutz 2024, August 2024
35 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 15, 2024
36 *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Krisen-Grosslagen/Prepositioning/prepositioning_node.html* (letzter Zugriff: 11.03.2025)
37 Claudia Plattner, BSI, *https://www.linkedin.com/pulse/cyberaggression-hybride-bedrohungen-des-21-und-wie-wir-plattner-yu2ue* 16.02.2025 (letzter Zugriff: 05.03.2025)
38 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 65, 2024
38 OT Security Made Simple, Aus dem Tagebuch eines Pentesters, März 2025, *https://rhebo.com/de/podcasts/aus-dem-tagebuch-eines-ot-pentesters*

# Nehmen Sie Ihre OT-Sicherheit
## in die Hand


**Rhebo OT Security**
Umfassende Cybersicherheit
für industrielle
Steuerungsnetze


**Rhebo Industrial**
**Security Assessment**
Risikobewertung
und Schwachstellenanalyse


**Rhebo Industrial Protector**
OT-Angriffserkennung
mit OT-Monitoring
und Anomalieerkennung

www.rhebo.com | sales@rhebo.com | +49 341 3937900

OT SECURITY Made in Germany

INFORMATION SECURITY MANAGEMENT SYSTEM DNV ISO/IEC 27001

bitkom

CYBERSECURITY MADE IN EUROPE™
Initiated by ECSO. Issued by eurobits e.V.

Allianz für Cyber-Sicherheit

**Rhebo** OT Security Made Simple

Rhebo bietet einfache und effektive Cybersicherheitslösungen für die Netzleit-, Fernwirk- und Steuerungstechnik sowie verteilte industrielle Anlagen in Energieunternehmen, Kritischen Infrastrukturen und Industrieunternehmen. Das deutsche Unternehmen unterstützt Kunden auf dem gesamten Weg der OT-Sicherheit von der initialen Risikoanalyse bis zum betreuten OT-Monitoring mit Anomalie- und Angriffserkennung. Rhebo ist seit 2021 Teil der Landis+Gyr AG, einem global führenden Anbieter integrierter Energiemanagement-Lösungen für die Energiewirtschaft mit weltweit rund 7.500 Mitarbeiter:innen in über 30 Ländern. Als vertrauenswürdiges Cybersicherheitsunternehmen ist Rhebo nach ISO 27001 zertifiziert sowie Partner der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und offizieller Träger des Gütesiegels »Cybersecurity Made In Europe«.

*www.rhebo.com*

**Rhebo GmbH** Spinnereistraße 7 | 04179 Leipzig | Deutschland
**rhebo.com**