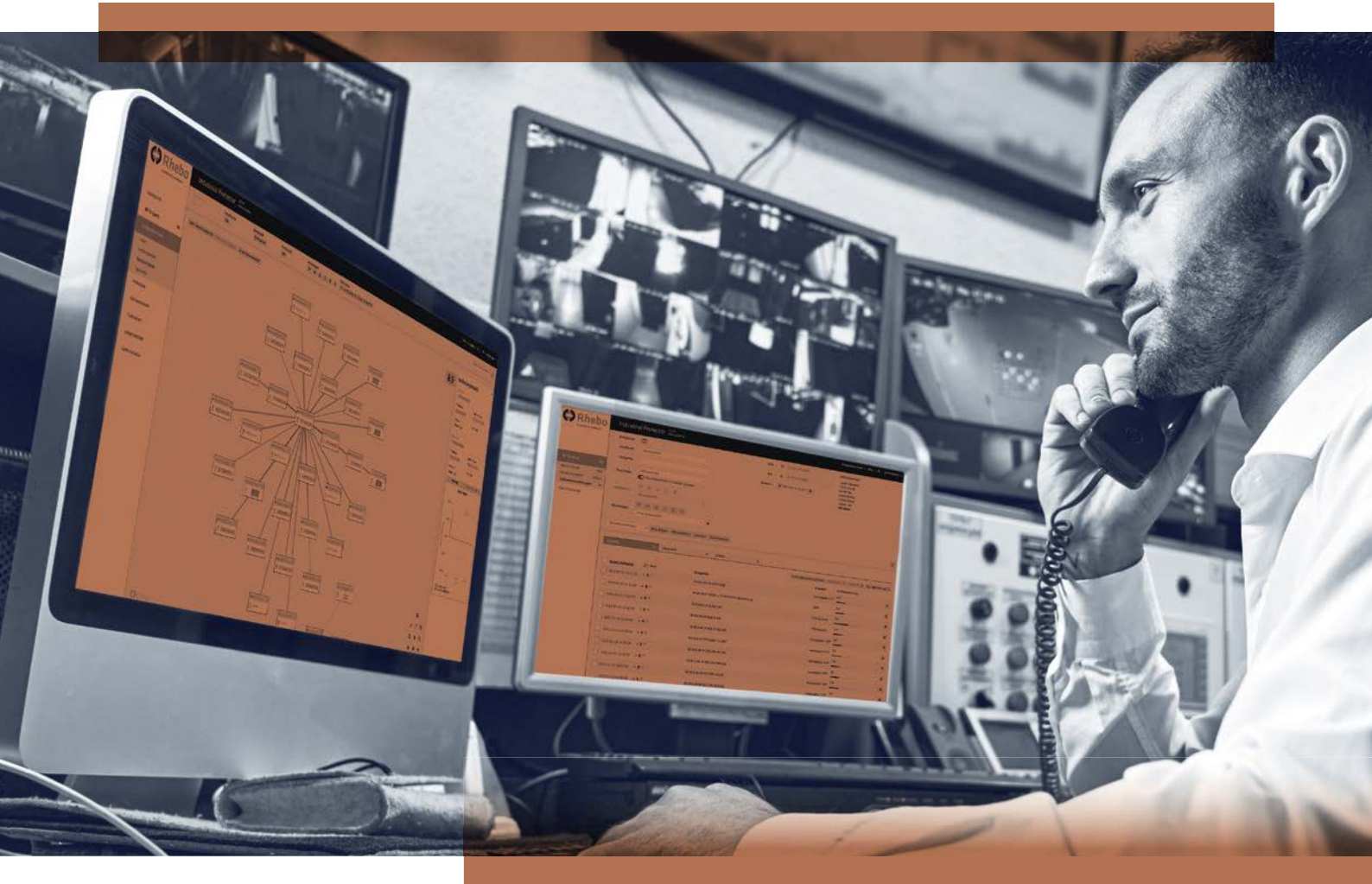


The state of OT cybersecurity 2024/2025

Metrics and trends from global to local



ENSURE NIS2
COMPLIANCE IN
YOUR OT



DETECT VULNERABILITIES
AND CYBER INCIDENTS
IN YOUR OT



BRIDGE
THE SKILLS GAP IN
OT SECURITY

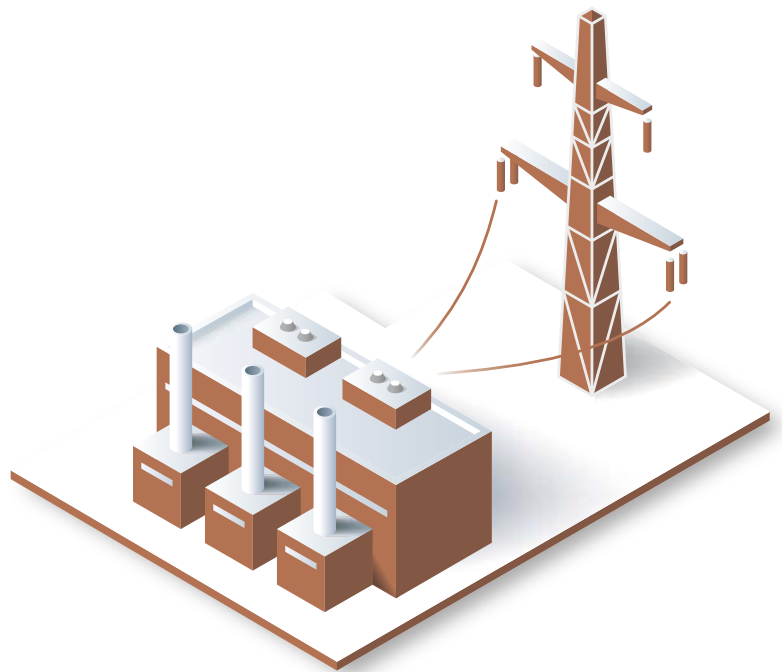
Executive Summary

OT cybersecurity has become an integral part of every cybersecurity strategy, and not just since the NIS2 directive and the national transposition laws. Cyber incidents, which in 2024 also led to a multitude of shutdowns in production systems and disruptions in critical infrastructure, have been highlighting for years how closely IT and OT, the digital world and physical processes, have become connected. With this level of networking, occupational safety and environmental protection increasingly emerge as aspects of a company's cybersecurity.

Even if direct attacks specifically targeting OT systems appeared to be only a handful in 2024, the risk landscape continues to evolve rapidly – from living-off-the-land methods to the growth of info-stealers and access brokers that systematically harvest data for later network penetration. 2024 was also a record year (again) for vulnerabilities in industrial components and systems. Geopolitical conflicts and cybercrime are increasingly going hand in hand. Pre-positioning activities by state-sponsored advanced persistent threats (APT) were and are only one indication of how strategically and sustainably adversaries operate and optimize their positions. The ever-increasing number of attacks on IT and the growing intercon-

nectedness between IT and OT continue to escalate the risks in OT as well. The results of Rhebo Industrial Security Assessments, during which existing security risks in OT networks are identified, also illustrate the open flanks of industrial infrastructure. Whether legacy protocols, outdated and incomplete authentication methods or OT components that automatically and unnoticed connect to the internet via factory settings: OT offers more than one attack vector. The fact that only a few major incidents worldwide have made it into OT can only be explained by the fact that the classic attack vectors (into IT) are still more lucrative and accessible for adversaries.

This report summarizes developments and information on cybersecurity in industrial companies. The data situation is not nearly as consistent as individual reports suggest. For example, due to slow reporting and evaluation processes, much of the data for 2024 incidents is incomplete and will continue to change (i.e. expand) in the coming months. The report tracks the metrics and trends from the global to the European to the German perspective and concludes with specific observations from Rhebo's field experience.



Contentlist

The global perspective on OT cybersecurity	3
The European perspective on OT cybersecurity	6
The German perspective on OT cybersecurity	8
The Rhebo perspective on OT cybersecurity	10
Ready for effective OT security?	13

The global perspective on OT cybersecurity

Metrics

Reports on cyberattacks that affected OT are **relatively inconsistent** depending on where the analysts draw the line. According to public reports, only 76 of reported cyberattacks impacted physical processes in 2024 (an increase by 300% since 2020, nonetheless), though they **affected approximately 1,076 industrial sites** (up by nearly 1,000% since 2020).¹

76
reported OT-related
cyber incidents

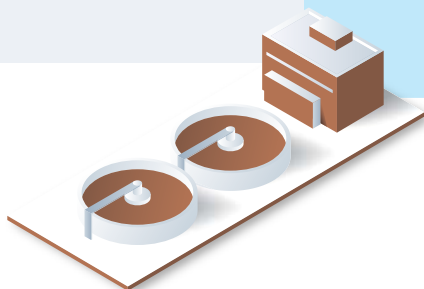
However, worldwide surveys interviewing CISOs and their respective security management show that 50 to 70% of cyberattacks on industrial companies also had an **impact on OT through »spillover«**. Of these, 20 to 38% even impacted **occupational safety and plant availability** increasing the scope of cybersecurity to the physical world.^{2,3}



Critical infrastructure is playing an ever-greater role among the cyberattack victims that must follow legal reporting obligations. According to statistics, of the 732 global incident reports analyzed in **2024**, a total of **418 affected critical infrastructure companies**⁴ (as of March 10, 2025). Due to delayed reporting and analyses, further incidents are regularly added to the statistics.

57
percent of victims are
critical infrastructure

Since strict reporting requirements and public availability exist in only a relatively small number of countries, the **number of unreported cyber incidents is likely to be considerably higher** than the official numbers. On April 1, 2025, Switzerland has become the latest country to make cyber incident reporting mandatory underlining a trend that hopefully will make future incident data more reliable.⁵



Overall, the global economy views the cyber risk landscape as increasingly complex. **45% of CISOs** surveyed by the World Economic Forum **fear disruption of operations the most**. There are many reasons for this:

- Geopolitical crises are making attacks as part of hybrid warfare ever more likely.
- Complex, often opaque supply chains increase both the likelihood of vulnerabilities and the risk of supply chain compromise.



45

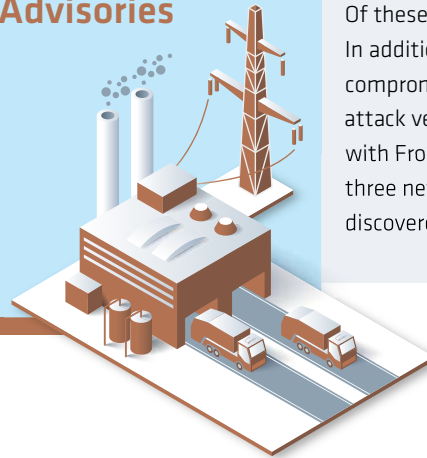
percent fear
operational disruption

- The rapid (and often untested) application of new technologies increases the risk of security gaps.
 - In OT/IoT, the CIA triad (confidentiality, integrity and availability) is extended into the realm of occupational and environmental safety.
 - The shortage of skilled cybersecurity personnel will increase by a further 8%.⁶
- These reasons will not disappear in the coming years – on the contrary.

OT components and systems remain insecure by design more often than not. In particular, older versions, which in OT may have lifecycles of 10–20 years, are **prone to vulnerabilities and persistent security gaps**. The US Cybersecurity and Infrastructure Security Agency (CISA) published a total of 432 ICS advisories on newly discovered vulnerabilities and threats in 2024, an **increase of 8.8 percent** from 2023.

432

ICS
Advisories



However, the majority of **cyberattacks** affecting industrial environments still occurred **via IT**, for whose components and systems over **33,000 vulnerabilities** were reported between July 2023 and June 2024 – **36% more** than in the same period the previous year.⁸ Of these, 76% were network-exploitable. In addition, remote access and supply chain compromise are increasingly being used as attack vectors (Figure 1).⁹ Additionally, with FrostyGoop, IOControl and Fuxnet, three new OT-capable malware variants were discovered in the wild in 2024.

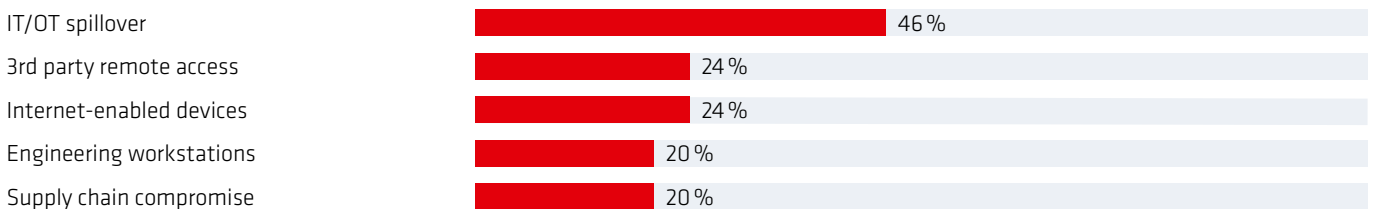


Figure 1 Top 5 initial attack vectors on industrial companies

Trends in cyberattacks

The tactics, techniques, and procedures (TTPs) of adversaries are becoming more sophisticated. At the same time, the red line of critical infrastructure has been crossed for several years now by cybercriminals and state-sponsored attackers. For example, in October 2024, American Water fell victim to a cyberattack. The largest US water and wastewater company supplies 14 million US citizens and 18 military facilities¹⁰. According to initial reports, the attack only affected the billing system, but it illustrates the trend that critical infrastructure companies are no longer being spared.

In February 2024, CISA and a number of intelligence agencies warned of the danger of prepositioning. According to their report, certain Advanced Persistence Threats (ATPs) are no longer aiming for immediate disruption, but rather long-term, strategic prepositioning as well as evasion and persistence at neuralgic points in the respective networks. The aim is to be able to strike immediately in the event of a potential geopolitical conflict¹¹.

Notably, so-called living-off-the-land techniques (LOTL) are increasingly being used, in which the given infrastructure is exploited without introducing additional payloads and malware.¹² In addition, cases have been uncovered in which North Korean actors infiltrate companies as remote IT workers under false identities and locations, steal data and blackmail the companies.¹³

Edge networking devices and remote access technologies are increasingly coming into focus as attack vectors – in 2024, these included components from Juniper, Sophos, Ivanti, Cisco, PaloAlto, Fortinet, FortiGate and Citrix¹⁴. In many cases, targeted zero-day vulnerabilities were exploited.¹⁵

Nevertheless, there were only a handful cyberattacks in 2024 that appeared to target OT infrastructure directly. Typically, corporate IT was either the main victim or the source of disruptions in OT (spillover). However, it must be kept in mind that the lack of hard numbers could be due to a number of factors, including:

- incorrect attribution of attacks,
- a lack of visibility in the OT and thus a lack of intrusion detection in OT (see interview p. 12),
- lack of reporting of incidents due to a deficient infrastructure and processes as well as security concerns about public disclosure.

Trends in OT cybersecurity

On the defensive side of OT security, two opposing trends are emerging. On the one hand, OT networks are becoming increasingly open. IT/OT convergence, cloud integration, remote access and control, and the integration of artificial intelligence are significantly reducing the past air gap between OT and the outside world and corporate IT.

On the other hand, OT security is still struggling with inherent limitations such as legacy systems, high-privilege access for service provid-

ers and manufacturers¹⁶, a lack of segmentation and visibility. At the same time, network intrusion detection systems (NIDS) are becoming more and more established as a tool for OT security¹⁷. In 2024, the North American Electric Reliability Corporation (NERC), which devises mandatory standards for the energy sector amongst others, proposed a new standard, CIP-015, that explicitly defines the requirements for network security monitoring.¹⁸ The standard will presumably become mandatory in the course of this year.

»The discussion on the commercial side is not fully fair for the OT because sometimes you are investing in safety and the protection against things not to happen. The understanding of the consequences of breaches is something else. This person, the OT CISO, or the organization, are going to help in translating this message to the corporate.«

Mohammed Adel Saad | Chief IT OT Cybersecurity Advisor, innovAKT

from the OT Security Made Simple podcast:

»How to translate IT into OT security?«¹⁹



The European perspective on OT cybersecurity

Metrics

The data for cyber incidents in the EU is much less conclusive due to **significant delays** in reporting at the EU level. While more than 1,200 incidents were reported to ENISA by the national CSIRTs for 2023, only 230 reports for 2024 were documented as of February 11, 2025. On March 11, 2025, this number had already risen to 575 – and counting. Of these, **34% have been attributed to malicious actors** so far.²⁰

3.000
attacks
on industrial
companies

By contrast, the European Union Agency for Cybersecurity (ENISA) recorded a total of **9,800 cyber incidents in the EU between July 2023 and June 2024**. About a third of these impacted industrial companies (Figure 2). They identify DDoS, ransomware, data theft, malware and social engineering as **the top 5 threats**.²¹ In the UK, the number of incidents reported to the National Cyber Security Centre (NCSC) had already **increased by 50% year-on-year by October 2024**.²²



The shortage of skilled labor remains one of the biggest challenges for companies in the EU as well. **Almost two-thirds** of companies reported **difficulties in finding qualified personnel** when filling vacancies.

70
percent
struggle with the
skills gap

76% of those employed in cybersecurity also have no formal qualifications or certification in the field. The **skills gap** therefore rose from 8th to **2nd place among the biggest cyber risks** in 2024.²³

Trends in cyberattacks

The ENISA assesses the cyber risk for Europe overall as »substantial«. This means that there is a high probability of attacks and that the disruption of essential and important entities is considered a realistic possibility.²⁴ In this context, ENISA has observed a further development of TTPs, which is comparable to global observations. Adversaries are increasingly relying on stealthy attacks that are not detected by firewalls and virus scanners. In addition to LOTL tech-

niques, fileless malware and zero-day exploits, these also include supply chain compromise (especially open-source libraries) and stolen credentials.²⁵ Information stealer software and access brokers continued to grow during the reporting period.²⁶ ENISA estimates that supply chain attacks due to (often opaque) software dependencies will pose the greatest cyber risk in coming years.²⁷

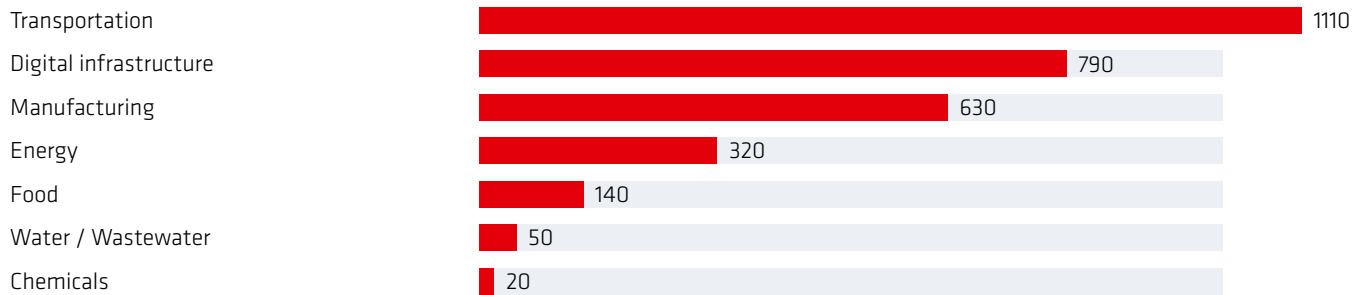


Figure 2 Distribution of sectors affected by cyberattacks in the EU 2023/2024

Trends in OT cybersecurity

In terms of cybersecurity, 2024 was an important year for the EU. Not only was the NIS2 directive transposed into national law – with a few exceptions, including Germany – obliging over 400,000 companies across the EU to ensure comprehensive cybersecurity. The Cyber Resilience Act also makes integral cyber security mandatory for all importers of products with a digital interface. In practice,

however, some companies (including critical infrastructure) still have a long way to go. Both the shortage of skilled workers and the lack of budgets and prioritization for cybersecurity – especially in supply chain assessment – make it difficult to ensure cyber resilience in many companies.²⁸

»With all the EU directives on resilience and security, companies are of course faced with a massive bucket load of compliance issues. Still, I would say that you're playing Russian roulette if you try to sit it out for as long as possible.«

Gerald Krebs | TÜV Information Technology

from the OT Security Made Simple podcast: »Ignoring NIS2 compliance is Russian roulette.«²⁹



The German perspective on OT cybersecurity

Metrics

The German Federal Office for Information Security (BSI) estimates that **22 APTs were active in Germany in 2024**. These primarily targeted government agencies and companies in the fields of foreign affairs, defense, public security and utilities.³⁰ However, the **total number of adversaries** targeting Germany **was 144**. This puts Germany in second place worldwide, behind the United States (264 adversaries).³¹

#2
of countries attacked

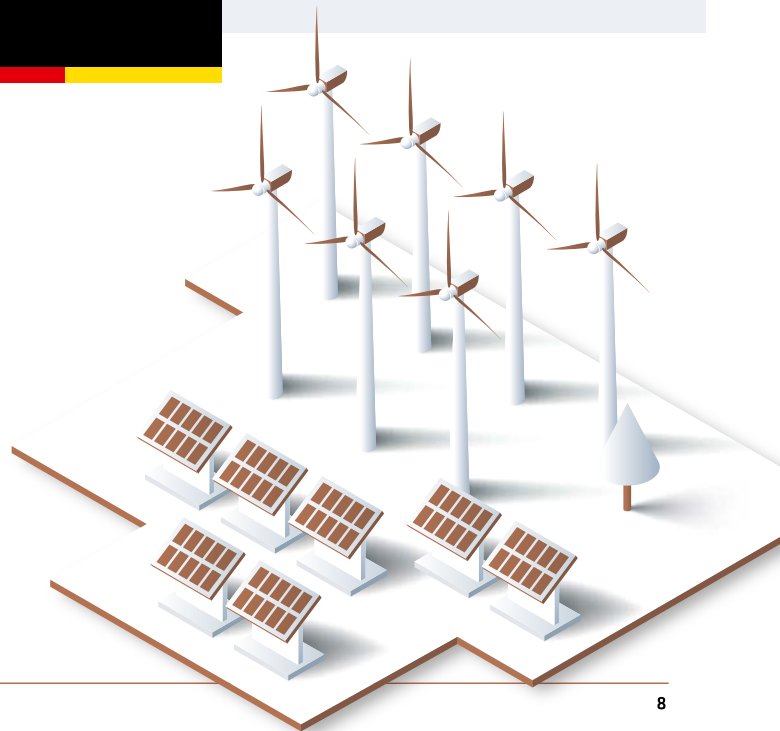


Between July 2023 and June 2024, the BSI received a **total of 726 incident** reports under the IT Security Act. Of these, 137 were in the energy sector, 185 in the transport and logistics sector, and 22 in the water sector. Among the attacks, several pro-Russian phishing campaigns were particularly noteworthy, as was the successful attack on PSI, a German manufacturer of control centers for energy supply systems.³²

The number of daily new **malware variants** **rose by 26%** during the BSI reporting period³³, significantly increasing the pressure on corporate cybersecurity and signature-based intrusion detection systems.

309
thousand
new malwares
daily

The business damage caused by cyberattacks totaled almost €179 billion. Of this, **€54.5 billion** (2023: €35 billion) was due to **disruptions to IT and production systems (i.e. OT)**. The number of companies affected by cyberattacks increased by over 12%, while the sabotage of IT and production systems went up by 7%.³⁴



Trends in cyberattacks

The German trend is largely in line with European and global developments. Targeted attacks on edge and network devices and the number of reported vulnerabilities also increased in Germany. The BSI received 18 zero-day reports per month for products from German manufacturers. In 2024, CISA published 150 ICS advisories for Siemens components alone (Rockwell Automation came in second with 55 advisories).³⁵ In principle, these figures also have a positive side: known vulnerabilities can be eliminated, even though security patching is a challenge of its own in OT environments.

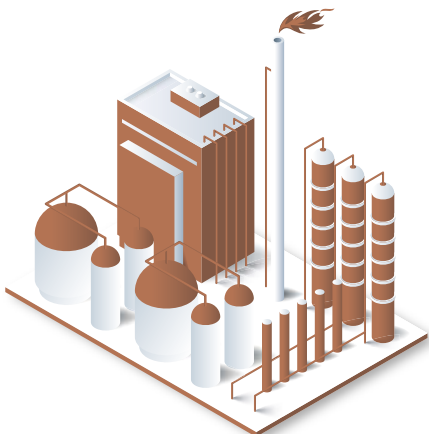
Compared to CISA, the BSI tried to play down the danger of prepositioning.³⁶ Whether this assessment is based on verifiable information

or a lack of visibility in many (not only OT) networks remains open for discussion. However, the President of the BSI, Claudia Plattner, showcased impressive foresight when she brought up the topic of cyber dominance («influence through digital products that give manufacturers access to information and functions») in addition to cybercrime and cyber conflict. She also assessed the lines between the three categories as fluid: »Today, criminal groups often act on behalf of the state. [...] Once an adversary is in the system, it's just two clicks from espionage to sabotage. It's even more dangerous when digital product vendors have persistent access to the systems their customers have installed, for example through regular updates.«³⁷

Trends in OT cybersecurity

With the delay of the NIS2 transposition law (NIS2UmsuCG), politicians have missed an important milestone for strengthening German cybersecurity and resilience. Nevertheless, the BSI rated the basic security level of critical infrastructures slightly better than in the previous year. According to the BSI, 140 out of 671 operators were able to improve the maturity level of their ISMS. Nevertheless, in the energy, water and transport sectors, 69% have still not implemented all the MUST requirements for an intrusion detection

system (IDS).³⁸ This is presumably mainly due to a lack of resources (know-how, time, personnel). Another reason could be that many companies still assume that firewalls and a security information and event management (SIEM) system constitute a high-performance, compliant IDS. However, these technologies not only leave crucial gaps, especially in the critical systems that actually require protection (i.e., the OT). They also generally lack functionalities such as network monitoring and anomaly detection.



IDS ACCORDING TO NIS2

Mapping of NIS2 requirements and Rhebo products & services

[Download poster](#)



Die Rhebo-Perspektive auf OT-Sicherheit

The insights presented here are aggregated results from Rhebo Industrial Security Assessments, in which the structure and communication of OT networks are analyzed for existing vulnerabilities and anomalies (Figure 3). They show that the challenges in OT security have remained largely unchanged over the years. Above all, they re-

veal legacy issues that need to be gradually eliminated. This is not surprising, since for almost all companies, a Rhebo Industrial Security Assessment is the first time their own OT perspective on cybersecurity and network quality is being addressed.

Metrics

In all the analyzed OT networks, **protocol-based security risks** were found. These include obsolete protocols such as **mDNS, LLNMR and SSDP** which are active but not needed or in real use in OT networks. Typically, obsolete protocols keep on running due to unchecked default settings. Whilst this is not a security issue itself,

100
percent
vulnerable protocols

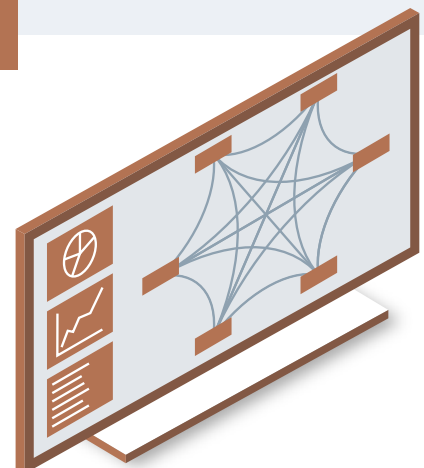
obsolete protocols pose an **easy-to-exploit attack vector** for adversaries. Furthermore, outdated protocol types like deprecated TLS, TFTP or HTTP remain a threat in OT networks. These protocols usually have **no or very weak security mechanisms** and can be easily exploited for **spoofing**.



Due to long lifecycles in the OT networks, **insecure authentication methods** were identified in 100% of all assessments. In 62.5% of all analyzed OT networks, the authentication method dated back to the 1990s and had long been breached. All OT networks used one or more protocols that do not provide any authentication at all.

100
percent
insecure authentication

Furthermore, OT communication still regularly used protocol types that send **passwords in plain text** and therefore were vulnerable to spoofing. In some cases, systems were identified in OT networks that did not support **any form of authentication**.



The proportion of **vulnerable software, firmware and operating systems** has fallen by 37%, but – at 63% – remains a challenge in terms of the attack surface due to unpatched known vulnerabilities. Connections and attempted connections from OT systems to the internet were found in 3 out of 4 companies. In some cases, systems were even **visible from the Internet**.

63
percent
vulnerable systems

In half of all assessments, devices were identified in the OT that are either uncharacteristic or inappropriate for industrial networks. They represented either a potential gateway for **espionage** due to **opaque security design** (e.g. Chinese switches) or outdated protocols, or a potential source for **network disruption** due to communication incompatible with ethernet requirements.

Inconsistencies in time synchronization of systems were **still common**. These can have several detrimental effects on OT networks:

- disrupt authentication,
- hinder forensic analysis of log files after an attack,
- affect real-time communication processes.

88
percent
unreachable devices or networks

On the stability side of OT network operation, **ICMP unreachable notifications** remained a common sight found in 88% of all assessments. They often correlate with other detected anomalies like retransmissions. Those alerts can be attributed to both, legit maintenance processes but also network or device deterioration or failures, hence providing **insights about the network quality**.

TYPICAL SECURITY RISKS IN OT

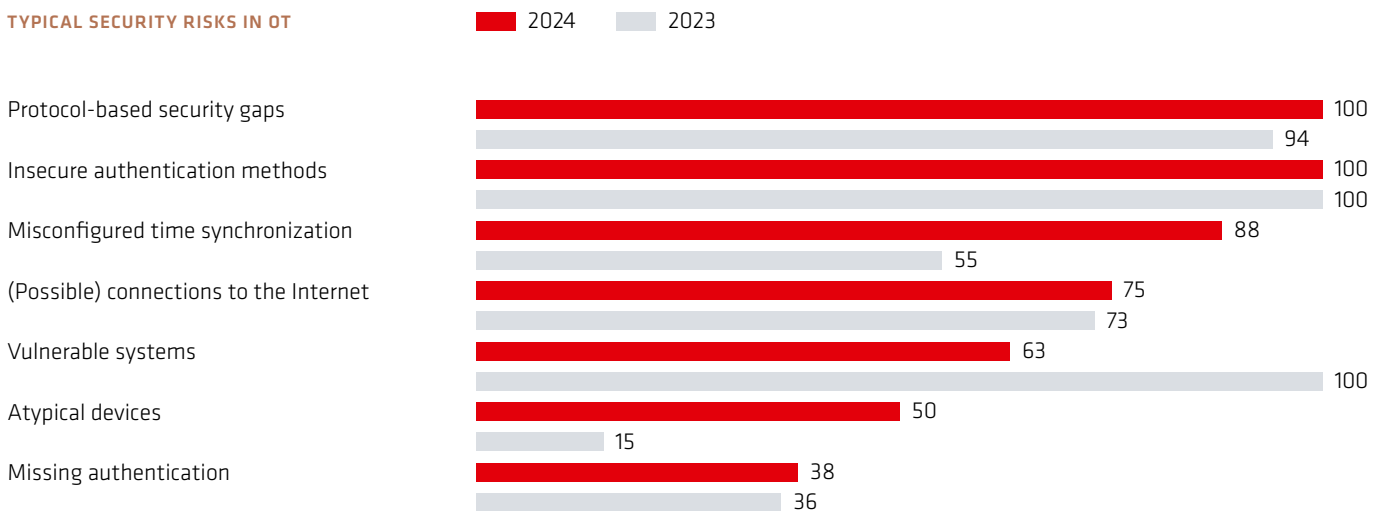


Figure 3 Development of the most common OT security risks between 2023 and 2024

Trends in OT cyberattacks

The results from Rhebo Industrial Security Assessments and the support provided to companies as part of Rhebo Managed Protection suggest that the companies currently do not face any concrete security incidents in the OT. However, they confirm that the operators are standing on an extremely complex – albeit for the time being potential – battlefield that is full of open flanks. Without net-

work security monitoring, new devices, connections and communication still fly under the radar of those in charge. This is a particular risk in industrial environments, where a large number of different players, including system integrators, system vendors and maintenance service providers, often have extensive access privileges.

Trends in OT cybersecurity

Awareness of the necessity of OT security has grown in recent years due to the expanding risk landscape. The intention of Rhebo's customers is clear: when installing a network intrusion detection system, it is not only about legal compliance, but also about real cybersecurity. Nevertheless, OT cybersecurity remains a new field in many companies, riddled with uncertainties. Security officers and engineers are usually still at the beginning of their journey. Visibility, clarity and

documentation of the existing OT infrastructure and usage (including that of 3rd party service personnel) are paramount. Rhebo customers therefore regularly draw on the expertise of the Rhebo customer service to evaluate and cross-check reported anomalies and to advise on appropriate measures. This active knowledge transfer and on-the-job training approach has helped to ensure that OT security expertise has grown steadily in the supported companies.

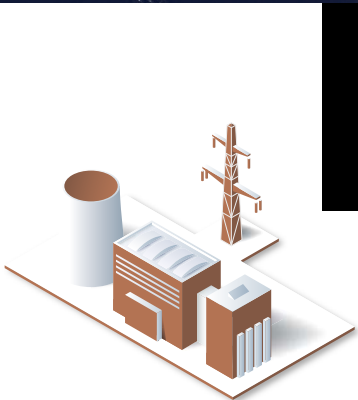


»There is a lack of people, a lack of technology and often a lack of understanding. For example, a few months ago a customer connected a power plant to the electricity exchange. This involved linking ABB and Siemens control systems. The service providers who look after the systems got it up and running within a day. That made me sit up and take notice. When I asked about the documentation and the network plans, I was told that they were still waiting for it, but that everything was already up and running. So we went there and took a look. Network cables were simply routed to fit the situation. The IP addresses were set up without any documentation. We were able to work out the system passwords relatively quickly and then write values down to the PLC. And that happens quite often.

The fact that many incidents are not reported is simply because they are not seen. There is a significantly higher number of unreported incidents at facilities that should actually report incidents but simply don't have the infrastructure, either technically or procedurally, to report such incidents.«

Patrick Latus | Independent Pentester for OT

From the OT Security Made Simple podcast: »From the diary of an OT pentester.«³⁹



Ready for effective OT security?

1



The first easy step
to OT security:

Rhebo Industrial Security Assessment

Cybersecurity starts with visibility.

The **Rhebo Industrial Security Assessment** is an OT cyber risk and vulnerability analysis that provides a deep understanding of your ICS / OT assets, risk exposure as well as recommendations for effective measures for hardening the systems.

You profit from

- the identification of all devices and systems within the OT including their properties, firmware versions, protocols, connections and communication behavior (Asset Discovery & Inventory);
- an in-depth analysis of existing CVE-documented vulnerabilities;
- the identification of risk exposure, security gaps and technical error states;
- a detailed audit report and workshop with actionable recommendations.

2



The seamless transition
to comprehensive OT security:

Rhebo Industrial Protector

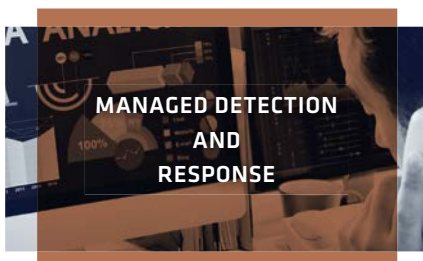
Cybersecurity does not end at the network perimeters.

The OT monitoring with next generation OT threat and intrusion detection **Rhebo Industrial Protector** provides enterprise-ready OT-dedicated security. It advances the existing perimeter firewall security by integrating holistic anomaly detection that does not interfere with the critical industrial processes.

You profit from

- real-time visibility of communication behavior of all OT and ICS assets (protocols, connections, frequencies);
- real-time reporting and localization of events (anomalies) that indicate cyberattacks, manipulation or technical error states;
- early identification of attacks via backdoors, previously unknown vulnerabilities and internal adversaries that firewalls fail to detect (defense-in-depth).

3



The recipe to peace of mind.
We monitor so you don't have to:

Rhebo Managed Protection

Cybersecurity needs resources and know-how.

With **Rhebo Managed Protection**, we support you in operating the OT security monitoring with anomaly detection, in particular in evaluating and responding to incidents, as well as continuously reviewing and improving mitigation mechanisms.

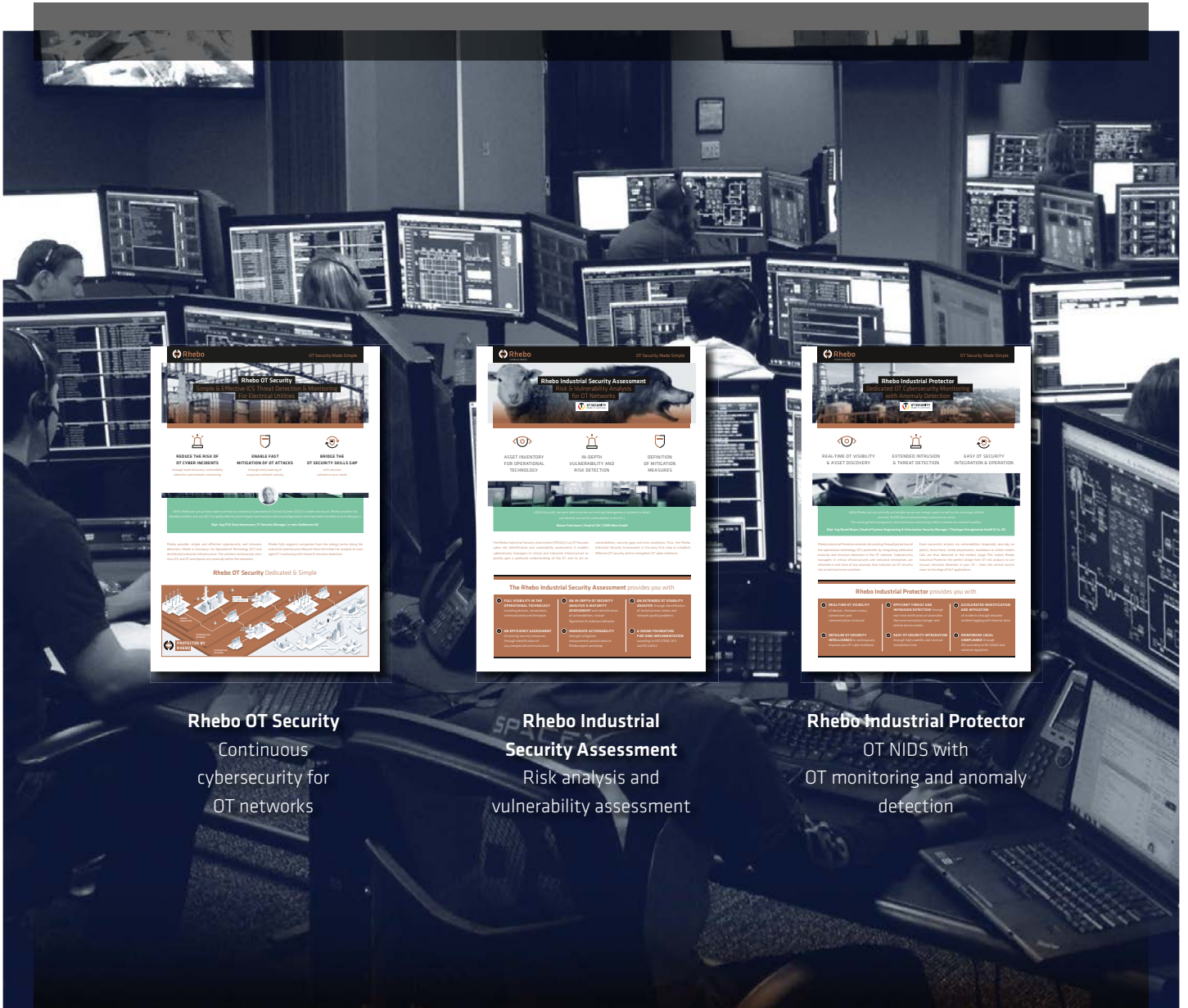
You profit from

- expert support for the operation of the OT security monitoring system;
- fast forensic analyses and assessment of OT anomalies;
- fast actionability in case of incidents;
- regular OT cyber risk analyses and maturity assessments for continuous improvement.

Sources and literature

- 1 2025 OT Cyber Threat Report, Waterfall, January 2025
- 2 SANS Research: SANS 2024 State of ICS / OT Cybersecurity, October 2024
- 3 ABi Research: State of OT Security, March 2024
- 4 European Repository of Cyber Incidents, January 2024 – December 2024, <https://eurepoc.eu/table-view> (last accessed March 3, 2025)
- 5 <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-104400.html> (last accessed March 17, 2025)
- 6 World Economic Forum: Global Cybersecurity Outlook 2025, January 2025
- 7 CISA ICS Advisories 2024 (last accessed March 10, 2025)
- 8 ENISA: Threat Landscape 2024, September 2024
- 9 SANS Research: SANS 2024 State of ICS / OT Cybersecurity, October 2024
- 10 CNN: <https://edition.cnn.com/2024/10/08/business/american-water-cyberattack-hnk-intl/index.html> October 2024 (last accessed February 10, 2025)
- 11 CISA: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, February 2024
- 12 CISA: Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance, February 2024
- 13 Bill Toulas: Undercover North Korean IT workers now steal data, extort employers, BleepingComputer, October 2024
- 14 Lawrence Abrams: The biggest cybersecurity and cyberattack stories of 2024, BleepingComputer, January 2025
- 15 <https://www.hackmageddon.com/2024/04/22/cves-targeting-remote-access-technologies> (last accessed February 11, 2025)
- 16 ABi Research: State of OT Security, March 2024
- 17 SANS Research: SANS 2024 State of ICS / OT Cybersecurity, October 2024
- 18 <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-015-1.pdf> (last accessed February 10, 2025)
- 19 OT Security Made Simple, How to translate IT into OT security?, January 2025
<https://rhebo.com/en/podcast/how-to-translate-it-in-ot-security> (last accessed March 11, 2025)
- 20 <https://ciras.enisa.europa.eu> (last accessed March 11, 2025)
- 21 ENISA, Threat Landscape 2024, p.14-16, September 2024
- 22 <https://therecord.media/uk-nationally-significant-cyberattacks-ncsc-horne-warning>, (last accessed February 12, 2025)
- 23 ENISA, 2024 Report on the state of cybersecurity in the union, p. 49, December 2024
- 24 ENISA, 2024 Report on the state of cybersecurity in the union, p. 14, December 2024
- 25 ENISA, Threat Landscape 2024, p. 58-59, September 2024
- 26 ENISA, Threat Landscape 2024, p. 30, September 2024
- 27 <https://www.enisa.europa.eu/topics/cyber-threats/foresight> (last accessed February 2, 2025)
- 28 ENISA, 2024 Report on the state of cybersecurity in the union, pp. 49-54, December 2024
- 29 <https://rhebo.com/en/podcast/ignoring-nis2-compliance-is-russian-roulette> (December 2024, last accessed March 11, 2025)
- 30 BSI, The state of IT Security in Germany 2024, p. 9, 2024
- 31 Forescout, 2024 Threat Roundup, p. 22, 2024
- 32 BSI, The state of IT security in Germany in 2024, p. 63 & 66, 2024
- 33 BSI, The state of IT security in Germany in 2024, p. 15, 2024
- 34 Bitkom, Economic protection 2024, August 2024
- 35 BSI, The state of IT security in Germany in 2024, p. 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 (last accessed March 11, 2025)
- 37 Claudia Plattner, BSI, <https://www.linkedin.com/pulse/cyberaggression-hybride-bedrohungen-des-21-und-wie-wir-plattner-yu2ue>
16.02.2025, (last accessed: 05.03.2025)
- 38 BSI, The state of IT security in Germany in 2024, p. 65, 2024
- 39 OT Security Made Simple, From the diary of a pentester, March 2025 <https://rhebo.com/en/podcast/from-the-diary-of-an-ot-pentesters>

Take your OT security into your own hands



Rhebo OT Security
Continuous cybersecurity for OT networks

Rhebo Industrial Security Assessment
Risk analysis and vulnerability assessment

Rhebo Industrial Protector
OT NIDS with OT monitoring and anomaly detection

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



Initiated by ECSSO. Issued by eurubits e.V.

Rhebo OT Security Made Simple

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The German company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. Since 2021, Rhebo is part of the Landis+Gyr AG, a leading global provider of integrated

energy management solutions for the energy industry with around 7,500 employees in over 30 countries worldwide. As a trustworthy cybersecurity provider, Rhebo is ISO 27001 certified, and was awarded the »Cybersecurity Made In Europe« label for its strict data protection and data security policies.

www.rhebo.com