NIS2 in OT-Netzwerken

Handlungsfähigkeit sicherstellen und Restrisiko managen

NIS2-COMPLIANCE IN DER OT SICHERSTELLEN

SCHWACHSTELLEN UND SICHERHEITSVORFÄLLE IN DER OT ERKENNEN

FACHKRÄFTEMANGEL IN DER OT-SICHERHEIT ÜBERBRÜCKEN

Einleitung

Die europäische NIS2-Direktive wird spätestens am 17. Oktober 2024 für einige Bewegung in Unternehmen sorgen. Bis dahin muss die Direktive für Cybersicherheit in Kritischen Infrastrukturen und (besonders) wichtigen Einrichtungen in deutsches Recht überführt werden. Für alle Unternehmen, die bereits das novellierte IT-Sicherheitsgesetz (IT-SiG 2.0) umsetzen mussten, gibt es eine gute Nachricht: Sie erfüllen bereits einen Großteil der Anforderungen. In Teilen hat das IT-SiG 2.0 die kommende NIS2 vorweggenommen. Dennoch geht NIS2 ein paar Schritte weiter. Die NIS2 trifft aber auch vor allem Unternehmen, die bislang nicht unter das IT-Sicherheitsgesetz fielen. Insgesamt versechsfacht sich die Anzahl der Unternehmen, für die eine sattelfeste Strategie und Umsetzung der Cybersicherheit zur gesetzlichen Pflicht wird.

Im Bereich der industriellen Netze – der Prozessleittechnik, Steuerungstechnik, Leit- und Fernwirktechnik – geraten viele Unternehmen angesichts des umfassenden Anforderungskatalogs und der baldigen Umsetzungspflicht unter Druck. Industrielle Cybersicherheit ist für die meisten ein neues Feld mit einigen Unterschieden zur IT-Sicherheit in Bezug auf Zielsetzung und technische Möglichkeiten. Die nach NIS2 zu erfüllenden Maßnahmen werden Unternehmen organisatorisch und technologisch mitunter an den Rand der Handlungsfähigkeit bringen.

Dieses eBook untersucht, welche Auswirkungen die aktualisierte europäische Richtlinie zur Netz- und Informationssicherheit (NIS2) auf Unternehmen (oder Einrichtungen, wie sie in der Richtlinie genannt werden) haben wird. Das eBook startet mit einer kurzen Einordnung der NIS2-Direktive in das größere Framework der Europäischen Cybersicherheitsstrategie. In Kapitel 2 werden die praktischen Einschränkungen erörtert, denen viele Unternehmen bei der Umsetzung der Anforderungen in der OT begegnen werden. Insbesondere wird auf das dadurch entstehende Restrisiko eingegangen. Kapitel 3 erläutert, wie diese Einschränkungen überwunden und das Restrisiko der realen Handlungsfähigkeit unter Kontrolle gebracht werden können. Abschließend gibt Andreas Könen vom BMI Tipps, welche Schritte Unternehmen vornehmen sollten.

Inhalte des Whitepapers

Die EU denkt Cybersicherheit größer

Die NIS2-Direktive wirft derzeit für viele Unternehmen große Wellen. Jedoch sollte sie nicht als einzelne Regulierung betrachtet werden. Sie ist eingebettet in ein größeres Cybersicherheits-Framework, das aktuell in Europa entsteht (Abbildung 1). Nicht zuletzt der Cyber Resilience Act (CRA) macht dies deutlich. Wird der Act so verabschiedet, wie am 12. März 2024 vom EU-Parlament bestätigt, wird Cybersicherheit zum Bestandteil jedes CE-Konformitätsprozesses. Produkte und Software, die digital kommunizieren, müssen damit automatisch cybersicher sein. Ergänzt wird das Framework durch die EU Direktive zur Resilience of Critical Entities (RCE), welche die physische Sicherheit und Resilienz kritischer Infrastrukturen in den Mittelpunkt stellt.

Die NIS2 Directive wird in Deutschland durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in geltendes nationales Recht überführt. Die EU RCE Directive wird durch das KRITIS-Dachgesetz implementiert. Beide deutschen Gesetze werden zum 17. Oktober 2024 verpflichtend.[1] Die EU versucht, über NIS2, CRA und RCE möglichst viele Aspekte der sicherheitsbezogenen Resilienz gesetzlich zu verankern. So verpflichtet NIS2 nicht nur zur Aufrechterhaltung der eigenen unternehmerischen Cybersicherheit. Mit dem Einbinden der Lieferkette werden auch Unternehmen von NIS2 indirekt betroffen sein, die nicht unter den direkten Geltungsbereich fallen. Diese ganzheitliche Strategie wird durch die Erweiterung der CE-Konformitätserklärung logisch erweitert. Sie bringt die von der NIS2-Richtlinie direkt betroffenen Einrichtungen jedoch mitunter an den Rand der effektiven Handlungsfähigkeit (siehe Kapitel 2).

EUROPA			
	The EU's Cybersecurity Strategy for the Digital Decade (2020)		
EU NIS Directive (2016) Cybersicherheit	**EU NIS 2 Directive** (2022) Cybersicherheit	**Cyber Resilience Act** (2022) Cybersicherheit als Teil der CE-Konformitätserklärung	**EU RCE Directive (CER)** (2022) Physische Sicherheit und Resilienz
DEUTSCHLAND			
IT-SiG (2015) **IT-SiG 2.0** (2021)	**NIS2UmsuCG** (2024)		**KRITIS-Dachgesetz** (2024)
Änderte **BSIG** und **EnWG**	Ändert **BSIG** und **EnWG** Ersetzt **IT-SiG 2.0**		
BSI-KritisV	**BSI-KritisV**		Zusätzliche Verordnungen
Orientierungshilfe »Einsatz von Systemen zur Angriffserkennung«	**Orientierungshilfe »Einsatz von Systemen zur Angriffserkennung«**		
Branchenspezifische Sicherheitsstandards (B3S)	**Branchenspezifische Sicherheitsstandards (B3S)**		
BETROFFENE UNTERNEHMEN IN DEUTSCHLAND			
Zirka 5.000 Unternehmen aus Energie, Wasser, Ernährung, Gesundheit, Transport und Verkehr, Entsorgung, IT und IK, Finanzen und Versicherungen	Zirka 30.000 Unternehmen aus Energie, Wasser und Abwasser, Ernährung, Gesundheit, Transport und Verkehr, Entsorgung, IT und IK, Finanzen und Versicherungen, Weltraum, Post/Kurier, Chemie, verarbeitendes Gewerbe, digitale Dienste, Forschung, Zentralregierung	Hersteller und Importeure von Produkten oder Software mit der Möglichkeit einer Daten- oder Netzwerkverbindung	Zirka 8.000 Unternehmen aus Energie, Transport und Verkehr, Finanz-/Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, IT und TK, Weltraum, Siedlungsabfallentsorgung, Zentralregierung

Abbildung 1 Übersicht der Gesetzespyramide zur Cybersicherheit Kritischer Infrastrukturen (Quelle: openkritis).

1 Stand März 2024 deutet sich aus politischen Gründe eine Verzögerung um einige Monate an.

Dass Cybersicherheit zu einer immer wichtiger werdenden Verpflichtung für die Wirtschaft wird, zeigt sich auch in dem Zuwachs an Unternehmen, die von den neuen gesetzlichen Anforderungen betroffen sein werden. Das bislang ausschlaggebende IT-SiG 2.0 galt in Deutschland für rund 5.000 Unternehmen aus acht kritischen Sektoren. Das NIS2UmsuCG verpflichtet ab Oktober 2024 rund 30.000 Unternehmen aus 14 Sektoren zu einer ganzheitlichen Cybersicherheit. Während das IT-SiG 2.0 das Augenmerk auf kritische Prozesse und Anlagen setzte, wird das NIS2UmsuCG mindestens die IT- und OT-Infrastruktur umfassen, die grundsätzlich für die Erbringung der jeweiligen (Dienst)Leistungen erforderlich ist.

Aktuelle Informationen zur Entwicklung der Gesetzentwürfe, wie z. B. geltende Schwellenwerte und Änderungen, finden Sie unter: *https://www.openkritis.de*

Weiterhin strebt die EU eine Harmonisierung der Cybersicherheitsstandards an. Wie es aussieht, geht die Reise in Richtung ISO/IEC 62443, der umfassenden Standardfamilie zum Thema Cybersicherheit in vor allem industriell geprägten Unternehmen. Das lässt sich aus der Beauftragung des CLC/TC 65X Technical Committee im Jahr 2023 ableiten, die Harmonisierung der bestehenden Sicherheitsstandards zu erarbeiten. CLC steht für die Europäische Standardorganisation CENELEC. TC 65X ist die Verbindung zwischen CENELEC und dem IEC-Komittee TC 65. Letzteres zeichnet sich für die IEC 62443 Standardfamilie verantwortlich. Unternehmen sind somit gut beraten, sich frühzeitig mit dem IEC 62443 Standard auseinanderzusetzen.

»Mit dem KRITIS-Dachgesetz und dem NIS2UmsuCG wollen wir Unternehmen klare Maßgaben geben, wie sie sich sowohl in der physischen als auch in der digitalen Welt aufstellen sollen, so dass sie resilient sind und sie bestimmte Krisenlagen auch unbeschadet überstehen. Das ist ein Gesamtkonzept«.

Andreas Könen, Leiter der Abteilung für Cyber und Informationssicherheit beim BMI
im Rhebo-Podcast OT Security Made Simple: Was die NIS 2 Direktive für Industrieunternehmen bedeutet.

NIS2 Die Grenzen der Prävention

NIS2 behandelt insgesamt 13 Aspekte, in denen Unternehmen nachweislich ihre Cybersicherheit stärken müssen:

1. Schulungen in Cybersicherheit und Cyberhygiene
2. Personalsicherheit, Zugriffskontrolle und Anlagen-Management
3. Risikoanalyse und Sicherheit für Informationssysteme
4. Management von Schwachstellen
5. Multi-Faktor- und kontinuierliche Authentisierung
6. Kryptografie und Verschlüsselung
7. Sichere Kommunikation (Sprache, Video und Text)
8. Bewertung der Effektivität von Cybersicherheits- und Risiko-Management
9. Bewältigung von Sicherheitsvorfällen
10. Sichere Notfallkommunikation
11. Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
12. Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
13. Sicherheit in der Entwicklung, Beschaffung und Wartung

Hinzu kommen anspruchsvolle Meldepflichten, Nachweispflichten und Registrierungspflichten.

Grundsätzlich bilden die 13 Aspekte das täglich Brot eines funktionierenden Informationssicherheitsmanagementsystems (ISMS), welches das gesamte Spektrum von der Prävention über den Betrieb eines Sicherheitssystems bis zum Notfallmanagement abdeckt. Insbesondere die präventiven Maßnahmen sind IT-Sicherheitsbeauftragten, Cybersicherheits-Managern und -Managerinnen durchaus bekannt. Sie können in der OT jedoch häufig nur mit Einschränkungen effektiv umgesetzt werden, denn:

1. In der OT ist Cybersicherheit (Aspekte 3-9) ein völlig neues Feld.
2. Unternehmen haben nur bedingt Einfluss auf die Lieferkette (Aspekte 12–13).
3. Das Angebot an Fachkräften für OT-Cybersicherheit ist stark limitiert.

Blind Spot #1: Die OT an sich

Die OT an sich birgt bereits historisch gewachsene Engpässe, wenn es um die Cybersicherheit geht. Die wenigsten Komponenten in OT-Netzen sind sicher konzipiert. In industriellen Umgebungen steht seit eh und je die Kernfunktionalität der Verfügbarkeit und Effizienz im Mittelpunkt. Der Prozess soll kosteneffizient laufen. Entsprechend fehlen sowohl Sicherheitsmechanismen als auch zusätzliche CPU-Kapazität, um diese nachzurüsten. Lebenszyklen von 10–20 Jahren und schlecht dokumentierte Legacy-Programmierung erschweren den schnellen Austausch oder eine gezielte Aktualisierung. Hinzu kommt, dass die OT selten so gut inventarisiert und administriert wird, wie die IT. In den meisten Fällen sind OT-Netze eine Blackbox für die Betreibenden. So fehlt Unternehmen in der Regel auch Wissen über die Vielzahl bestehender Schwachstellen und Sicherheitsrisiken in ihrer OT (Abbildung 2).

TOP 10 SICHERHEITSRISIKEN IN OT-NETZWERKEN 2023

Ergebnisse aus Rhebo Industrial Security Assessments in 2023

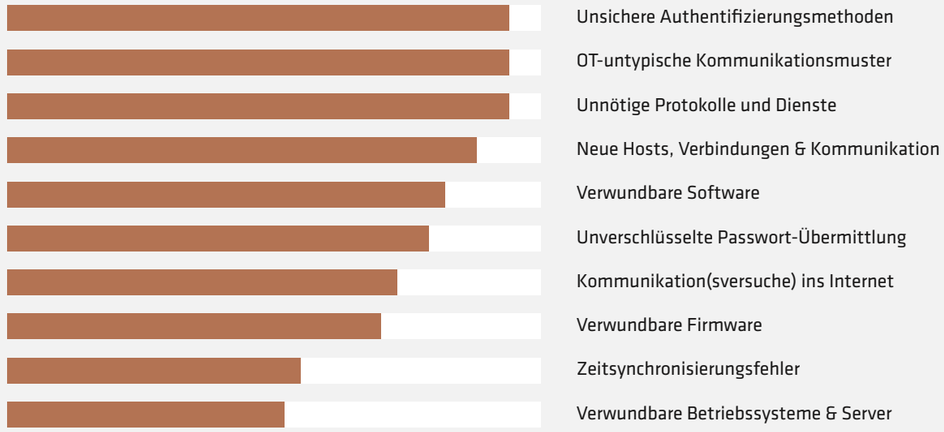


Abbildung 2 In OT-Netzen finden sich versteckte Sicherheitslücken auf allen Ebenen, wie die Ergebnisse der Rhebo Industrial Security Assessments 2023 bei Kunden zeigen.

Zudem gibt es sowohl organisatorische als auch technische Unterschiede zwischen IT und OT, so dass die aus der IT-Cybersicherheit abgeleiteten Anforderungen der NIS2 in der OT mitunter an Grenzen stoßen (Tabelle 1).

NIS2-ANFORDERUNG	KONFLIKT IN DER OT
Berechtigungs- u. Zugangsmanagement • Multi-Faktor-Authentifizierung (MFA) • Single-Sign-On (SSO)	SSO erfordert starke Systemintegration, die in der OT heutzutage selten gegeben ist. MFA erfordert, dass allen Mitarbeitenden eine sichere zweite Quelle der Authentifizierung zur Verfügung gestellt wird. Insbesondere beim Umgang mit den vielen Dienstleistungsunternehmen für Wartung, Instandhaltung und Services kann sich diese Anforderung schwierig gestalten.
Sichere Kommunikationskanäle	Wie auch in der IT ist dies ein zweischneidiges Schwert, da Unternehmen heutzutage größtenteils Plattformanbieter wie Google, Microsoft, Zoom oder Meta nutzen. Diese bieten zwar eine verhältnismäßig gute Sicherheitsfunktion, werfen aber u.U. datenschutzrechtlich aufgrund ihres US-amerikanischen Sitzes einige Fragen auf. Bei der Fernsteuerung von Anlagen bieten VPN-Verbindungen zwar ein Mindestmaß an Authentifizierung, sind jedoch leicht zu kapern und auszunutzen.
Verschlüsselte Kommunikation	In der Praxis ist das in der OT – häufig aufgrund von Echtzeitprozessen – bislang nur eingeschränkt möglich, auch wenn es immer mehr Angebote in dieser Hinsicht gibt. Viele OT-Protokolle bieten zudem keine Option zur Datenverschlüsselung.
Management von Schwachstellen	OT-Komponenten sind in der Regel »insecure by design«. Fast täglich werden neue Schwachstellen bekannt[2]. Gleichzeitig schränken Lebenszyklen, Fragen der Prozessstabilität und -kontinuität und lückenhafte Asset Inventories die zeitnahe Implementierung von Sicherheitspatches ein.
Risikoanalyse • Bewältigung von Sicherheitsvorfällen • Bewertung der Cybersicherheitseffektivität • Business Continuity Prozesse	Noch immer fehlt in OT-Netzen vor allen Dingen Sichtbarkeit – sowohl in Bezug auf die bestehenden Assets als auch bezüglich sicherheitsrelevanter Vorgänge.

Tabelle 1 Herausforderungen bei der Umsetzung der NIS2-Anforderungen in der OT

2 Die US-amerikanische Cybersecurity & Infrastructure Security Agency (CISA) veröffentlichte 2023 über 400 Advisories zu neuen Schwachstellen in OT-Komponenten.

Für das Vorfallmanagement nennt die NIS2 neben der Prävention explizit die Erkennung (detection) und die Reaktion auf Störungen (mitigation). Letzteres hängt logisch und chronologisch von einer gut funktionierenden Angriffserkennung ab, wie sie bereits im IT-SIG 2.0 gefordert ist. Und diese muss heutzutage über eine Firewall am Perimeter und ein alleinstehendes SIEM (als vermeintliche Wunderwaffe) hinausgehen.

Firewalls fehlt das Wissen über Zero-Day-Schwachstellen, also für die Cybersicherheit noch unbekannte Schwachstellen. Auch erkennen sie keine bösartigen Netzwerkzugriffe, die über authentische Zugangsdaten (credentials) erfolgen. Auswertungen der letzten Jahre zeigen einen Trend weg von Angriffen, die auf Schadsoftware basieren, zu Angriffen, die ohne diese auskommen. Zwischen 2018 und 2022 stieg der Anteil malware-freier (entdeckter) Angriffe von 39% auf 71%. Diese beruhen zu einem Großteil auf gestohlenen Zugriffsinformationen. Sind Angreifende erst einmal im Netzwerk, hilft keine Firewall mehr. Ein SIEM wiederum benötigt Unmengen von Daten, um Angriffsmuster zu erkennen und zu melden. Mit dem blinden Fleck in der OT, bleibt selbst mit dem besten SIEM ein Angriff in der Steuerungstechnik ungesehen.

Firewalls und SIEM-Systeme stoßen an ihre Grenzen bei:

1. neuartigen Angriffsmustern,
2. der Ausnutzung nicht gepatchter oder bislang unbekannter Schwachstellen,
3. der Ausnutzung gestohlener Zugangsdaten oder
4. Cyberangriffen über einen Supply-Chain-Compromise.

Blind Spot #2: Die Lieferkette

Unternehmen agieren nicht im luftleeren Raum. Sie arbeiten mit anderen Unternehmen zusammen, erwerben und nutzen Geräte und Applikationen von Drittanbietern und tauschen Daten mit der Außenwelt aus. Kurz: Jedes Unternehmen ist eng verzahnt mit und abhängig von anderen Unternehmen und Einrichtungen, deren Risikoexposition und Security Posture auf die eigene Cybersicherheit Einfluss haben (Abbildung 3).

Wie relevant und realistisch diese Faktoren sind, zeigen beispielsweise Supply-Chain-Compromise-Vorfälle wie Solarwinds (2020), Log4Shell (2021) und ViaSat SATCOM (2022) sowie die täglichen CISA Security Advisories für ICS-Komponenten. Supply-Chain-Compromise sind Cyberangriffe, bei denen Zuliefer- oder Dienstleistungsunternehmen attackiert werden, um an die eigentlichen Zielunternehmen zu gelangen.

Abbildung 3 Bei der Vielzahl von Drittanbieter-Komponenten in der OT reicht ein unsicheres Gerät für die Netzwerk-Penetration durch Supply Chain Compromise (Quelle: Pixabay)

Die NIS2 adressiert dieses durchaus reelle Problem mit zwei neuen Anforderungen:

- Cybersicherheit muss Kernaspekt beim Kauf von IT/OT-Systemen oder -Dienstleistungen sein.
- Cybersicherheit muss Kernaspekt bei der Auswahl von Zulieferunternehmen sein. Das soll sogar so weit reichen, dass beim Zulieferer eine sichere Produktentwicklung forciert werden soll.

NIS2 sieht sogar vor, dass besonders wichtige und wichtige Einrichtungen für bestimmte (noch zu definierende) Prozesse nur Produkte und Dienstleistungen einsetzen dürfen, die über eine Cybersicherheitszertifizierung verfügen.
Diese Anforderungen der NIS2 denken die Risikoexposition eines Unternehmens logisch und konsequent weiter. Sie adressieren die Gefahr, die von einer starken Vernetzung und dem blinden Vertrauen gegenüber Drittanbietern und Subunternehmen ausgeht.
In der Praxis kollidieren beide Anforderungen jedoch mit einer Realität, in der kooperative Cybersicherheit entlang der Lieferkette ein noch zu entdeckendes Fremdwort darstellt.

Ein Unternehmen hat nur bedingt Einfluss auf:

1. die Cybersicherheit der Lieferketten-Unternehmen,
2. die Cybersicherheit und Cyber-Awareness von Dienstleistungsunternehmen (z. B. Wartungsunternehmen, die in der OT arbeiten),
3. die Produktentwicklung in Zulieferunternehmen.

Das hat in der Praxis zwei Konsequenzen für Unternehmen:

1. Die Auswahl an zur Verfügung stehenden Systemen, Geräten, Applikationen und Dienstleistungen wird sich (zumindest mittelfristig) stark einschränken. Das ist in Deutschland bereits bei der Auswahl von Smart Metern der Fall, die im Gegensatz zu anderen Ländern einer Sicherheitszertifizierung (in Deutschland durch das BSI) bedürfen. Rein theoretisch dürften Unternehmen, die unter NIS2 fallen, dann nur noch mit Subunternehmen zusammenarbeiten, die ein ISMS nach ISO 27001 betreiben oder die IEC 62443 umgesetzt haben.
2. Um nicht komplett handlungsunfähig zu sein – denn mal ehrlich: Welche OT-Systeme und -Komponenten würden Sie als sicher bezeichnen? – müssen unsichere Geräte und Systeme während des Betriebs (noch) stärker überwacht werden. Das gilt insbesondere bei kritischen Systemen und Komponenten.

Die technischen und prozessbedingten Einschränkungen in der OT sowie die mindestens mittelfristig nicht komplett umsetzbare Supply Chain Security bedeuten, dass die Prävention von Cybervorfällen nur sehr bedingt in OT-Umgebungen umgesetzt werden kann. Der Trend geht deshalb von der reinen Prävention zur kontinuierlichen Überwachung und Detektion als zweite Frontlinie der Cybersicherheit. Auch das hat die NIS2 im Blick.

Blind Spot #3: OT-Sicherheits-Personal

Laut des Instituts der Deutschen Wirtschaft (IW) werden bis 2027 zirka 128.000 qualifizierte Arbeitskräfte in den Digitalisierungsberufen fehlen[3]. Der Bitkom e.V. spricht sogar schon von 149.000 offenen Stellen in diesem Jahr[4]. Im Durchschnitt bliebe eine Stelle für IT-Fachkräfte inzwischen bis zu 7 Monate unbesetzt.

Diese Prognose setzt sich im Bereich Cybersicherheit fort. Bereits 2022 hatte sich die weltweite Lücke zwischen Bedarf und Angebot zum Vorjahr um 26 Prozent vergrößert, trotz eines Zuwachses an Sicherheitsexpert:innen von 10 Prozent[5]. In einer Studie des IDC im September 2022 stellten fast zwei Drittel aller Befragten fest, bereits einen akuten Fachkräftemangel in der Cybersicherheit ihrer Unternehmen zu erleben[6]. In einer deutschen Umfrage sehen 40 Prozent der CISOs den Mangel an qualifizierten Fachkräften als größtes Problem, die Cybersicherheit im Unternehmen zu gewährleisten[7]. Derzeit existieren zwar keine konkreten Zahlen, die den Bedarf an Fachpersonal in die Bereiche IT-Sicherheit und OT-Sicherheit unterteilen. Der Leidensdruck in der OT-Sicherheit dürfte aber noch einmal höher liegen. Schließlich stellt der Bereich für den Ausbildungsmarkt und die meisten Unternehmen noch ein völlig neues Feld dar. Und NIS2 erhöht den Druck weiter.

Mit NIS2 steigt mit einem Schlag die Anzahl der gesetzlich zu Cybersicherheit verpflichteten Unternehmen in Deutschland von rund 5.000 auf 30.000! Diese Unternehmen müssen binnen kurzer Zeit neues Know How aufbauen und ihr Cybersicherheitsmanagement erweitern. Angesichts der gesetzlich verankerten Haftbarkeit der Geschäftsführung bei diesem Thema braucht es effektive, praktische und schnell umsetzbare Lösungsansätze.

3 *https://t3n.de/news/it-fachkraeftemangel-berufe-handeringend-gesucht-1610463*
4 *https://www.bitkom.org/Presse/Presseinformation/Deutschland-fehlen-137000-IT-Fachkraefte*
5 *https://www.isc2.org/research*
6 *https://www.idc.com/getdoc.jsp?containerId=prEUR149854222*
7 *https://www.csoonline.com/de/a/mehrheit-der-deutschen-cisos-klagt-ueber-mangelnde-unterstuetzung,3674574*

Die Restrisiken in den Griff bekommen

Die guten Nachrichten sind, dass Unternehmen die Blind Spots durchaus in den Griff bekommen können, ohne intern alle bestehenden Strukturen auf den Kopf stellen zu müssen.

Dafür ist ein geringfügiger Paradigmenwechsel in der Cybersicherheit sinnvoll. Der etablierte Ansatz der Prävention und Abwehr an Netzwerkgrenzen und Endgeräten wird durch Sichtbarkeit und Detektion von Abweichungen innerhalb der Netzwerke ergänzt. Dieser Perspektivenwechsel ist entscheidend, denn in der heutigen dynamischen Risikolandschaft ist keine 100%-ige Cybersicherheit mehr möglich. Im Gegenteil, das nicht zu beseitigende Restrisiko einer Kompromittierung des Netzwerks wächst. Entsprechend braucht es Wege, mit dem Restrisiko zu leben und es unter Kontrolle zu halten. Und Kontrolle erfolgt über Sichtbarkeit.

Mit der Unsicherheit der OT und der Lieferkette umgehen

Ein leistungsstarkes Werkzeug, um das Restrisiko durch die notorisch unsichere OT und die schwer beeinflussbare Lieferkette unter Kontrolle zu bekommen, ist ein netzwerkbasiertes OT-Angriffserkennungssystem (OT-NIDS) mit integriertem OT-Monitoring und Anomalieerkennung. Die Anomalieerkennung untersucht die OT-Kommunikation nicht auf bekannte schadhafte Signaturen (das erledigen Firewalls und SIEM-Systeme), sondern auf Vorgänge, die vom bestehenden, etablierten Muster abweichen. Das ist in der OT möglich, da industrielle Anlagen durch sich wiederholende, vorhersehbare Kommunikation geprägt sind. Aktivitäten von Angreifenden sind deshalb relativ leicht von der legitimen Kommunikation unterscheidbar. Entscheidend ist zudem, dass das OT-Angriffserkennungssystem die Kommunikation innerhalb des Netzwerkes überwacht (Abbildung 4).

Dadurch sieht das Angriffserkennungssystem auch Angreifende, die über neuartige Angriffstechniken, unbekannte Schwachstellen, gestohlene Zugangsdaten und Supply Chain Comprimise in die OT gelangt sind, ohne die Firewalls und das SIEM-System in Alarm versetzt zu haben.

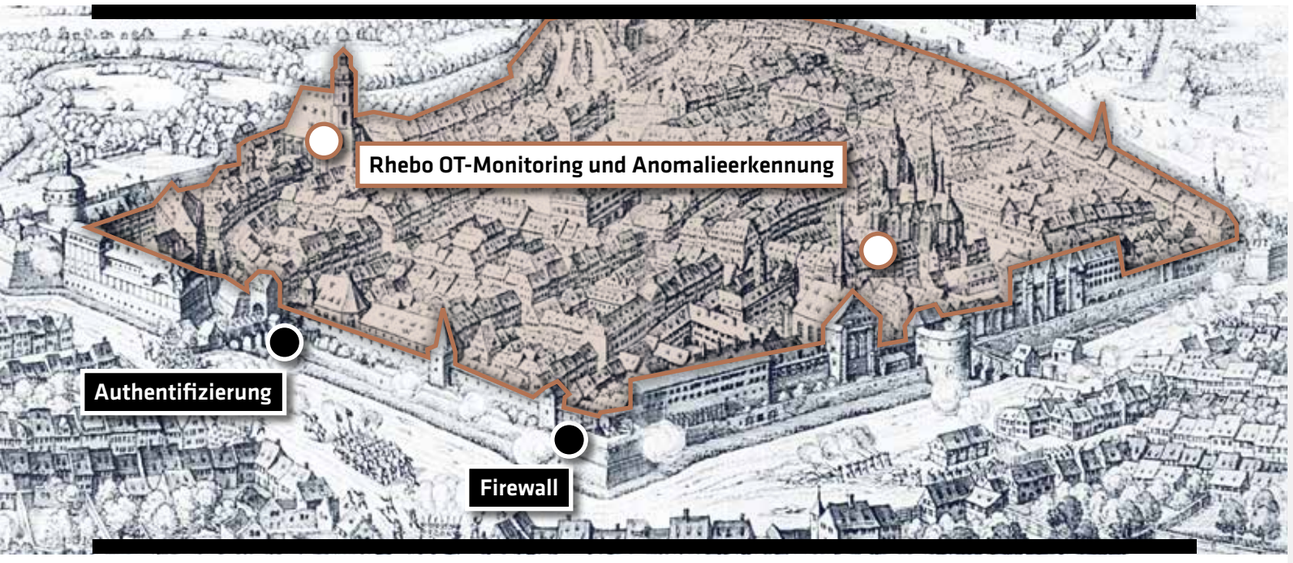


Abbildung 4 Ein OT-Netzwerk muss wie eine Stadtfestung gesichert sein. Dazu gehört auch die Innere Sicherheit.

Da die Anomaliemeldung in Echtzeit erfolgt, können die Sicherheitsverantwortlichen umgehend reagieren. Im Durchschnitt benötigen Angreifende 84 Minuten zwischen Erstzugriff und lateraler Bewegung auf ein weiteres Gerät. Solange Sicherheitsteams der etablierten 1-10-60-Regel (1 Minute fürs Erkennen, 10 Minuten fürs Verstehen, 60 Minuten fürs Reagieren) folgen können, haben sie somit eine Chance.

Die Sichtbarkeit und dadurch entstehende Handlungsfähigkeit und Risikokontrolle (als Teil des geforderten Risikomanagements) entstehen durch die OT-Angriffserkennung über vier aufeinander aufbauende Stufen. Diese finden sich auch in den Kernanforderungen der NIS2.

1. Eine **Risikoanalyse** schafft Klarheit darüber, welche Cybergefahren für ein Unternehmen bestehen und welche Gewichtung diesen jeweils zu geben ist. Zu diesem Wissen gehört nicht nur, welche Gefahren (z. B. aktuelle Schadsoftwaretypen) von außen bestehen. Vielmehr beinhaltet es ein Verständnis darüber, welche Sicherheitslücken, Schwachstellen und internen Cyberrisiken (z. B. durch Konfigurationen, informelle Workarounds und Funktionsweisen von Drittanbieter-Systemen) bestehen. Rhebo-Kunden starten deshalb immer mit einem Rhebo Industrial Security Assessment, bei dem die OT eingehend auf bestehende Schwachstellen und Sicherheitslücken untersucht und parallel das Asset Inventory erstellt wird.
2. Ein klares **Asset Inventory** gewährleistet, dass Unternehmen wissen, welche Geräte und Systeme wo und in welcher Art im Einsatz sind. Schließlich kann nur geschützt werden, was als schützenswert bekannt ist. Ein OT-NIDS wie Rhebo Industrial Protector schafft hier klare Sicht. Es liest passiv – also ohne die OT in irgendeiner Form zu belasten – jegliche Kommunikation innerhalb der OT mit und erstellt daraus eine detaillierte Netzwerkkarte (Abb. 5). In dieser werden alle Geräte und Systeme mit ihrem Kommunikationsverhalten, Metadaten und Verbindungen dargestellt und Hinweise gegeben, wenn für eine Komponente Schwachstellen bekannt sind.
3. Im laufenden Betrieb erhalten die Sicherheitsmanager:innen vom OT-NIDS eine Echtzeitmeldung von Anomalien in der OT-Kommunikation. Um das Sicherheitsteam bei der Einschätzung und Maßnahmenfindung zu unterstützen, werden die identifizierten Anomalien automatisch mit einer Risikobewertung versehen. Diese erlaubt die gezielte Priorisierung und die **frühzeitige Erkennung** einer Netzwerk- oder Gerätekompromittierung. Rhebo Industrial Protector arbeitet hierbei mit Deep Packet Inspection (DPI) Technologie, so dass auch Befehls- und Funktionsänderungen erkannt werden können.
4. Die Vorfalldokumentation erfolgt sowohl über die Anzeige aller Anomalien einzeln und in logisch zusammenhängende Vorfälle gruppiert, als auch über die Speicherung aller identifizierten Anomalien als packet capture (pcap). Sicherheitsverantwortlichen liegen damit alle Informationen zu einem Sicherheitsvorfall vor. Sie können somit gezielt den Weg und das Ausmaß eines Vorfalls analysieren und **Gegenmaßnahmen einleiten.** Außerdem unterstützt die Dokumentation bei der anspruchsvollen **Meldepflicht** an die Behörden.

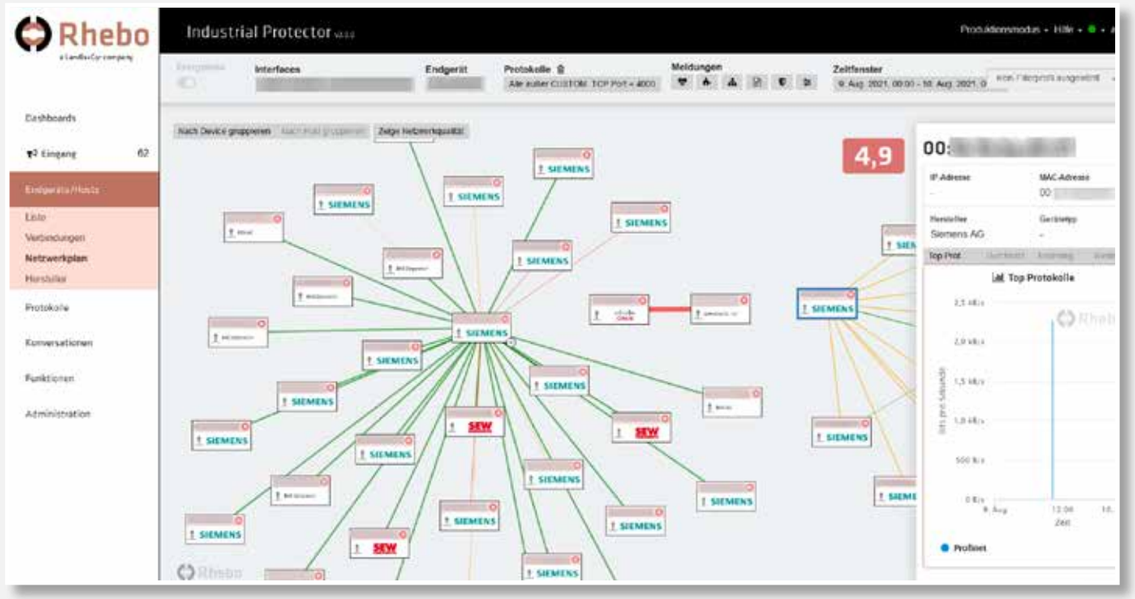


Abbildung 5 OT-Sicherheit basiert auf der Sichtbarkeit aller Assets im Netzwerk mit den dazugehörigen Eigenschaften

Wer überwacht die Überwachung?

Schließlich stellt NIS2 die Frage, wie eigentlich die Effektivität der eingesetzten Sicherheitssysteme nachgewiesen werden kann. Wie bereits gezeigt, sind Firewalls und SIEM wichtige Komponenten, haben aber auch ihre klaren Einschränkungen – insbesondere, wenn die OT betroffen ist. Aufgrund der Zunahme erfolgreicher Phishing-Kampagnen und bekannt gewordener Schwachstellen im OT-Bereich wird somit ein blindes Vertrauen auf die bestehenden Sicherheitsmechanismen selbst zu einem relevanten Risiko.

Das OT-NIDS mit Anomalieerkennung kann hier zusätzlich als »Wächter der Wächter« fungieren. Anomaliemeldungen geben letztlich immer Hinweise darauf, dass etwas im Netzwerk nicht richtig läuft. Damit zeigen sie auch an, wenn die bestehende Sicherheitsarchitektur Lücken aufweist, Angreifende in das Netzwerk eingedrungen sind oder Mitarbeitende Sicherheitsrichtlinien verletzen. Ein OT-NIDS wird somit zu einem zentralen Werkzeug, um zum einen dediziert die OT nach NIS2 abzusichern (Abb. 6) und zum anderen die vielen Restrisikolücken zu schließen.

Rhebo
a Landis+Gyr company

NIS2 COMPLIANCE IN OT-NETZWERKEN

NIS2-ANFORDERUNGEN	GRUNDLEGENDE SICHERHEITSZIELE*				
Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	Verfahren zur regelmäßigen Risikoanalyse und Schwachstellenbewertung einführen (z. B. nach IEC62443-3-3)	OT-Netzwerk und -Ökosystem kartieren einschließlich Asset Discovery und Beschreibung	Bestehende Schwachstellen Sicherheitslücken und Cyberrisken im OT-Netz identifizieren	Sicherheitsmaßnahmen entsprechend der Ergebnisse festlegen	ISO 27001 umsetzen
Bewältigung von Sicherheitsvorfällen	End-to-end Anomalie- und Angriffserkennung umsetzen **	Angriffe, böswillige, fehlerhafte oder andere Aktivitäten im Netz, die sich auf kritische Dienste auswirken könnten, frühzeitig erkennen	Schnelle Reaktion auf Cybervorfälle sicherstellen (Incident Response) ermöglichen	Schnelle forensische Analyse und Abschätzung der Auswirkungen nach Vorfall sicherstellen	Schadsoftware und Angreifende an Netzwerkgrenzen bestmöglich abwehren (z. B. über Firewalls)
Aufrechterhaltung des Betriebs	Störung der industriellen Prozesse durch Sicherheitsmaßnahmen vermeiden	Business-Continuity-Plan erstellen	Mehrstufiges Backup-Management etablieren	Schnelle Notfallwiederherstellung ermöglichen	Professionelle Krisenbewältigung und -kommunikation einrichten
Sicherheit der Lieferkette	Zulieferunternehmen mit etablierten Cybersicherheitsrichtlinien präferieren	Least Privilege Access für Lieferanten etablieren	Sicheren Lieferanten-Zugang zum Netzwerk gewährleisten (z. B. VPN, sichere Passwörter)		
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen	Cybersicherheit von Drittanbieter-Software einfordern: Rhebo Industrial Protector	Cybersicherheit eigenentwickelter kritischer (I)IoT-Geräte und -Produkte sicherstellen	Cybersicherheit von Drittanbieter-Software sicherstellen (gilt für alle Komponenten in der OT)	Effektive und sichere behandlung und Offenlegung von Schwachstellen sicherstellen	
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Die Wirksamkeit des Cybersicherheit-Systems fortlaufend überpüfen und verbessern	Cybersicherheitslage und Risikoexposition regelmäßig neu bewerten			
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	Defense-in-Depth-Architektur aufbauen, um Versagen der Perimetersicherung frühzeitig zu erkennen	Gefährdete Anlagen überwachen, bei denen Patches/Aktualisierungen nicht möglich sind	Grundlegende Anforderungen für Sicherheitssysteme umsetzen (z. B. nach IEC62443-3-2)	Ausbreitung von Angriffen eindämmen (z. B. durch Netzsegmentierung, Verkehrsfilterung)	
	Unnötige Anwendungen (z. B. private Messenger) von OT-Systemen entfernen	Digitale Ressourcen in Bezug auf Firmware, Betriebssystem usw. auf dem neuesten Stand halten	Starke Passwortrichtlinien festlegen und umsetzen	Regelmäßige Cybersicherheitsschulungen für das Personal umsetzen	
Konzepte und Verfahren für den Einsatz von Kryptografie & Verschlüsselung	Sichere Kommunikation über sichere Protokolle gewährleisten	Verschlüsselte Übertragung von Passwörtern und anderen sensiblen Informationen sicherstellen			
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	Alle Assets (Geräte, Systeme, Anwendungen) erkennen und inventarisieren	Asset-Eigenschaften dokumentieren (inkl. ID, Anbieter, Verbindungen, Protokolle)	Rollenbasierten Zugang zu Systemen und Funktionen sicherstellen	Sicherheitsüberprüfungen und -sensibilisierung in das Einstellungs- und Vertragsvergabeverfahren integrieren	Unbefugten physischen Zugriff auf Assets verhindern
Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung	Personalisierte Multi-Faktor-Authentifizierung sicherstellen	Sichere digitale Kommunikation gewährleisten	Unbefugten Zugriff auf digitale Assets verhindern		
Berichtspflichten	Innerhalb von 24 Stunden nach einem Vorfall Frühwarnungan CSIRT *** übermitteln	Innerhalb von 72 Stunden erste Bewertung an CSIRT übermitteln (inkl. Aussagen zu Schweregrad, Auswirkungen, Quelle)	Auf Anfrage des CSIRT Aktualisierungen zum Status des Vorfallsmanagements bereitstellen	Innerhalb eines Monats detaillierten Bericht an das CSIRT übermitteln (inkl. Informationen zu Schweregrad, interne und grenzüberschreitende Auswirkungen, Ursache, Abhilfemaßnahmen)	

LEGENDE

- Direkte Umsetzung und Ermöglichung
- Monitoring und benachrichtigende Funktion im Falle von Vorgängen, die von den Sicherheitsrichtlinien abweichen
- Lösungen über Rhebo Trusted Partners verfügbar

* Die aufgeführten Ziele sind in der NIS 2 nicht explizit definiert, sondern spiegeln allgemeine grundlegende Sicherheitsziele wider, wie sie in internationalen Normen wie der IEC 62443 empfohlen werden.
** Verpflichtend für kritische Infrastrukturen in Deutschland nach IT-SiG 2.0
*** CSIRT (computer security incident response team) = behördliches Computer-Notfallteam

Abbildung 6 Übersicht, wie Unternehmen ihre NIS2-Konformität mit Rhebo-Leistungen und dem OT-NIDS Rhebo Industrial Protector abdecken können.

Dem Fachkräftemangel begegnen: OT-Sicherheit schrittweise ins Unternehmen holen

Trotz anhaltendem Fachkräftemangel haben Unternehmen einen effektiven Hebel, ihre OT-Kompetenz durch Managed Services und Training-on-the-Job aufzubauen.

Im ersten Schritt gilt es, kurzfristig Lücken zu schließen. Externe Expert:innen übernehmen hierfür den Betrieb der OT-Angriffserkennung, analysieren und bewerten die identifizierten Anomalien und informieren die Verantwortlichen im Unternehmen nebst Empfehlungen für Gegenmaßnahmen. Aufgrund der Empfindlichkeit industrieller Prozesse bleibt die Entscheidung und Durchführung der Gegenmaßnahmen dabei im Hoheitsgebiet des betroffenen Unternehmens. Die Sicherheitsbeauftragten im Unternehmen können aufgrund der Informationen schnell und gezielt reagieren.

Im zweiten Schritt wird intern eine Position für OT besetzt. Der Betrieb des Angriffserkennungssystems geht damit an das Unternehmen über. Das externe Cybersecurity-Serviceteam steht ab diesem Zeitpunkt als »Sparring-Partner« zur Verfügung. Sicherheitsvorfälle oder technische Fehlerzustände, die vom Angriffserkennungssystem in der OT identifiziert wurden, können so regelmäßig gemeinsam ausgewertet und Gegenmaßnahmen abgestimmt werden. Ziel ist der fundierte Wissenstransfer, um das interne Know How kontinuierlich aufzubauen und die Verantwortlichen sattelfest in OT-Sicherheit zu machen.

Der schrittweise Ansatz nimmt nicht nur den Druck aus der neuen Herausforderung der OT-Sicherheit. Durch den Fokus auf Wissenstransfer mit dem Aufbau eigener Kompetenzen bleibt auch der langfristige Investitionsrahmen planbar.

Kunden von Rhebo können im Rahmen von Rhebo Managed Protection zwischen drei Serviceleveln wählen (und diese bei Bedarf anpassen).

MANAGED OT SECURITY
Betriebsunterstützung
mit dem OT-NIDS bei
Stadtwerke Bochum Netz

Referenzstory herunterladen

Interview Was tun, wenn NIS2 droht?

Mitte 2023 interviewte Rhebo-Gründer Klaus Mochalski im Rahmen des Rhebo-Podcast *»OT Security Made Simple | Über die Notwendigkeit von NIS2, um Cybersicherheit voranzubringen«* Andreas Könen, Leiter der Abteilung für Cyber- und Informationssicherheit beim Bundesministerium des Innern und für Heimat. Dies ist ein Auszug aus dem Transkript.

KLAUS MOCHALSKI
Gründer von Rhebo

ANDREAS KÖNEN
Abteilungsleiter CI »Cyber- und IT-Sicherheit«
Bundesministerium des Inneren und Heimat

Klaus Mochalski
Was würden Sie Unternehmen auf den Weg geben, das Bewusstsein zu schärfen, dass NIS2 keine Bürde ist, sondern etwas, das für das eigene Geschäft essentiell ist?

Andreas Könen
Ich würde natürlich zunächst empfehlen, in die Cyber-Sicherheitslage einmal hineinzuschauen. Einfach mal beim BSI oder beim Bundeskriminalamt auch direkt nachzufragen und sich anzuschauen, welches Ausmaß allein schon all die Ransomware-Vorfälle mittlerweile annehmen. Das ist eine regelrechte Seuche. Und wer sich das klarmacht, sieht – egal welchem Geschäftszweck mein Unternehmen dient – dass er oder sie davon unmittelbar bedroht wird.

Klaus Mochalski
Was empfehlen Sie Unternehmen, die neu unter die NIS2-Anforderungen fallen und nun kurzfristig die Umsetzung bewerkstelligen müssen?

Andreas Könen
Die erste Sache ist, sich zu vergegenwärtigen, warum bin ich jetzt in diese Regulierung hineingefallen? Was bedeutet das? Was droht mir? Was muss ich jetzt als erste Schritte tun? Sicher ist eine juristische Anfangsberatung immer gut. Die kann man auch bei den Verbänden erhalten. Einfach um zu wissen, wie muss ich mich denn jetzt gegenüber der staatlichen Seite dabei äußern? Das BSI wird ebenfalls sichtbar nach außen tragen, wie dieser Prozess ablaufen soll. Und da würde ich sagen, nicht in Nervosität verfallen.

Der zweite Schritt ist dann der Inhaltliche. Ich muss schauen, ob es Standards gibt, die auf mich zutreffen. Gibt es schon etwas, was mir etwa ein Verband bieten kann? Gibt es irgendetwas, was mir mein IT-Dienstleister bieten kann? Auf den sollte man zügig zugehen und ihn konfrontieren mit dem, was kommt. Sie sollten Druck ausüben, zu sagen, was denn jetzt im Einzelnen zu tun ist.

Ja, und dann am Ende steht wirklich die Betrachtung, wie verhalte ich mich in einer Krise? Wie komme ich in ein vernünftiges IT-Krisen-Notfall-Management rein?

Also, die drei Schritte sind es insgesamt. Erstens klarmachen, was heißt NIS2 für mich und Kontakt zum BSI aufnehmen. Zweiter Schritt, meine eigene IT-Infrastruktur mit meinem IT-Dienstleister einmal durchdringen und drittens am Ende mich selbst nochmal aufstellen, wie ich im Fall eines Falles reagiere.

OT-Sicherheit in 3 Schritten

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

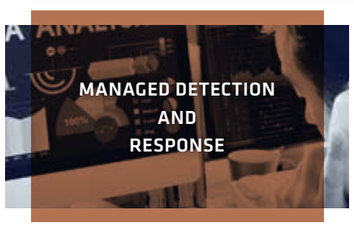
OT-Sicherheit endet nicht an den Netzwerkgrenzen.

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.

Setzen Sie NIS2 effektiv
und einfach in Ihrer OT um

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

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. Rhebo ist Partner der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Teletrust – Bundesverband IT-Sicherheit e.V.. Als vertrauenswürdiges IT-Sicherheitsunternehmen ist Rhebo nach ISO 27001 zertifiziert und offizieller Träger des Gütesiegels »Cybersecurity Made In Europe«. *www.rhebo.com*

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

EBOOK NIS2 | 03-2024 | © Rhebo GmbH