



# Echtzeitschutz und kontinuierliche Verbesserung der Energieversorgung bei der e-netz Südhessen AG



SICHTBARKEIT UND NACHVOLLZIEHBARKEIT IN DER FERNWIRKTECHNIK



SCHNELLE AUFKLÄRUNG VON ANGRIFFEN UND FEHLKONFIGURATIONEN



KONTINUIERLICHE VERBESSERUNG DURCH REGELMÄSSIGE AUDITS

»Mit Rhebo können wir nicht nur fundiert prüfen und nachweisen, dass unsere Netzleittechnik sicher und stabil läuft. Rhebo schafft uns auch den detaillierten Einblick in unsere Fernwirktechnik und Prozessnetzsteuerung, um sonst schwer sichtbare neuartige Angriffe und Fehlkonfigurationen schnell zu erkennen, einzugrenzen und zu beheben.«

Dipl.-Ing (TU) Sven Hanemann | IT-Sicherheitsbeauftragter | e-netz Südhessen AG



## Ausgangssituation und Herausforderung

Die e-netz Südhessen AG versorgt als Verteilnetzbetreiber der Entega AG rund eine Million Menschen in 63 Kommunen der Region Rhein-Main-Neckar zuverlässig mit Strom und Gas. Als nachhaltiger, zukunftsorientierter Energie- und Infrastrukturdienstleister steht die e-netz Südhessen dabei für einen zuverlässigen Betrieb und die innovative Weiterentwicklung ihrer Strom- und Erdgasnetze in Richtung Energiewende. Bereits seit 2010 setzt das Unternehmen hierfür ein Qualitäts-, Energie-, Arbeitsschutz- und Umweltmanagement nach ISO 9001, ISO 14001, ISO 45001 und ISO 50001 um.

Im Jahre 2012 erfolgte die Einführung eines zertifizierten Informationssicherheitsmanagements (ISMS) auf Basis des BDEW-Whitepapers. Um die Infrastruktur kontinuierlich zu verbessern und deren Ausbau optimal zu begleiten, soll die Netzleittechnik zukünftig regelmäßig auf Sicherheitslücken und Optimierungspotentiale überprüft werden. Weiterhin sollte ein System integriert werden, das die Fernwirktechnik und Prozessnetzsteuerung ganzheitlich gegen Störungen durch Cyberangriffe, Fehlkonfigurationen und technische Fehlerzustände absichert.



### Detektion von Angriffen und Fehlfunktionen

Datenkommunikation in Fernwirktechnik (IEC104) kontinuierlich und auf Wertebene überwachen, um kleinste Veränderungen frühzeitig zu erkennen und zu beheben.

### Schnelle, fundierte Analyse von Vorfällen

Alle Details zu Vorfällen dokumentieren, um diese nachvollziehen, fundiert analysieren und bezüglich Ort und Auslöser eingrenzen zu können.

### Sicherstellen der ISMS-Rezertifizierung

Umsetzen eines kontinuierlichen Verbesserungsprozesses sowie Überprüfung des Sicherheitslevels und der Maßnahmeneffektivität.

# Lösung

## RISIKOANALYSE

### Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit

- Assets und Kommunikationsstrukturen analysieren;
- Gefährdungen für Sicherheit und Stabilität bewerten;
- Maßnahmen definieren.

## NETZWERKMONITORING MIT ANOMALIEERKENNUNG

### Rhebo Industrial Protector

- kontinuierlich Fernwirktechnik und Prozessnetzsteuerung überwachen;
- Cyberangriffe, Sicherheitslücken, Schadprogramme und Fehlerzustände in Echtzeit identifizieren und analysieren.

## KONTINUIERLICHE VERBESSERUNG

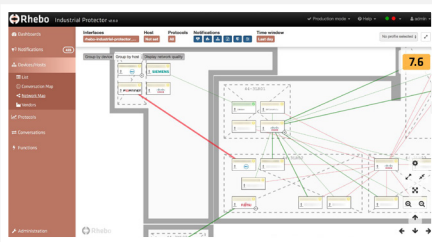
### Rhebo Managed Protection

- Regelmäßig Stabilitäts- und Sicherheitsaudits durchführen;
- Forensische Analyse von Vorfällen erleichtern;
- Notfallunterstützung einholen.

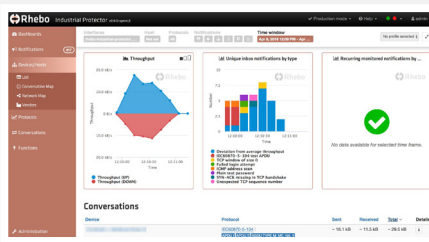
## Umsetzung und Erkenntnisse

Rhebo führte bei der e-netz Südhessen ein Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit der Fernwirktechnik und Prozessnetzsteuerung durch. Mittels drei passiver Sensoren wurde die Kommunikation über Ethernet, Mobilfunk und das Konzernnetz von Rhebo aufgezeichnet und analysiert. Die Ergebnisse zeigten eine sehr gut geführte und gesicherte Infrastruktur. Weitere Anwendungsfälle (z. B. Anschluss eines Umspannwerkes) wurden simuliert, um die Funktionalität der Netzwerkmonitoring-Lösung Rhebo Industrial Protector zu evaluieren. Die detaillierten Monitoringdaten, äußerst

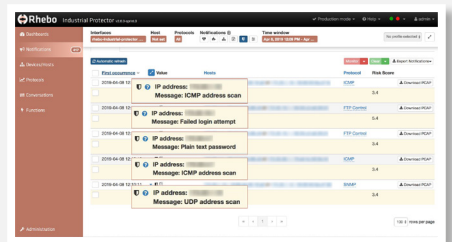
gute Nachvollziehbarkeit von Vorfällen sowie die individuelle Anpassung der Ergebnisdarstellung überzeugte die e-netz Südhessen, Rhebo Industrial Protector nachfolgend mit sieben Datenabgriffspunkten fest zu integrieren. In den kommenden Jahren unterstützt Rhebo die e-netz Südhessen zudem über ein Rhebo Managed Protection Service Level Agreement mit regelmäßigen Audits und forensischen Analysen bei der kontinuierlichen Verbesserung der Sicherheitsinfrastruktur sowie der Soforthilfe bei Vorfällen.



Die Netzwerkkarte inventarisiert alle Assets in der Fernwirktechnik mit ihren Eigenschaften und Verbindungen.



Zu jedem Host werden in Echtzeit Details wie Protokolle, Verbindungen und Anomalien angezeigt.



Rhebo Industrial Protector meldet unsichere Vorgänge wie Scans und unverschlüsselte Passwörter.

## Ergebnisse



**VOLLSTÄNDIGE TRANSPARENZ** über Struktur, Assets und Verbindungen der Netzleittechnik hergestellt.



**DATENKOMMUNIKATION IN FERNWIRKTECHNIK** lückenlos überwacht.



**ECHTZEITALARMIERUNG UND DOKUMENTATION** von Kommunikationsveränderungen sichergestellt.



**STABILEN BETRIEB** der Netzleittechnik gestärkt durch Identifikation von Fehlkonfigurationen.



**KONTINUIERLICHER VERBESSERUNGSPROZESS** nach ISO 27001 und ISO 9001 durch regelmäßige Risikoanalysen vorangetrieben.



**NACHVOLLZIEHBARKEIT UND RISIKOBEWERTUNG** von Vorfällen signifikant verbessert.

### 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 integrier-

ter 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 offizieller Träger des Gütesiegels »Cybersecurity Made In Europe«.

[www.rhebo.com](http://www.rhebo.com)