



# Rhebo AMI Security

## Effektive Cybersicherheit für die Advanced Metering Infrastructure (AMI)



### RISIKO VON AMI-CYBER-VORFÄLLEN REDUZIEREN

durch Kommunikationsüberwachung und Schwachstellenerkennung



### AMI-SCHÄDEN ABWEHREN

durch frühzeitige Warnung vor verdächtigen Aktivitäten



### FACHKRÄFTEMANGEL ÜBERBRÜCKEN

durch auf Sie zugeschnittene AMI-Sicherheits-Services



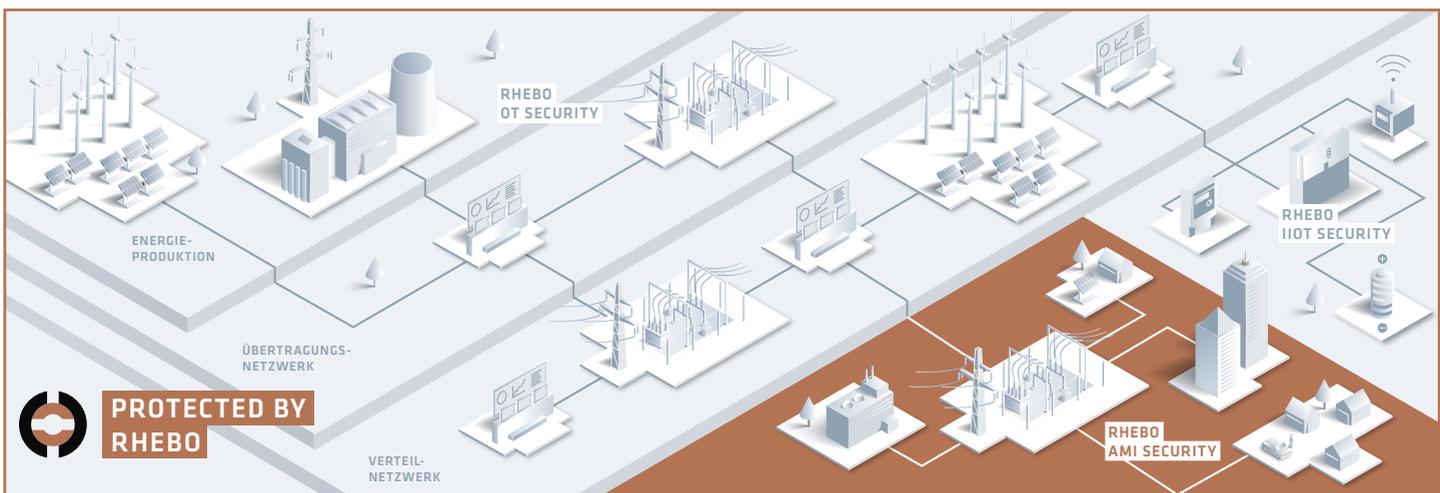
»Unser Ziel ist es, unseren Kunden eine leistungsfähige und sichere Advanced Metering Infrastructure zu liefern. Rhebo AMI Security bietet eine einfache und effektive Lösung, die wir schnell und über ein kosteneffizientes Abomodell in die Systemanwendungen unserer Kunden integrieren können«.

Juha Torstenson | Vice President für Software, Service & Solution | Landis+Gyr

Rhebo AMI Security lässt sich in Head End Systems (HES) integrieren und überwacht kontinuierlich die Kommunikation innerhalb der Advanced Metering Infrastructure (AMI), ohne dass Änderungen an der AMI-Architektur oder den Geräten erforderlich sind. Jede Anomalie innerhalb der AMI wird in Echtzeit erkannt, bewertet und gemeldet.

Selbstverständlich werden Unternehmen aus dem Energiesektor von Rhebo entlang des gesamten OT-Sicherheitslebenszyklus unterstützt – von der ersten Risikoanalyse bis zur betreuten AMI-Überwachung mit Erkennung von Angriffen und Anomalien.

## Rhebo AMI Security Gezielt & Einfach



## Smart Meter steigern millionenfach das Cyberrisiko

Der Smart-Meter-Rollout ist integraler Bestandteil der Energiewende und Digitalisierung. Allein in Europa soll die Anzahl der eingesetzten Smart Meter **bis 2026 auf 227 Millionen** steigen. In den USA waren im Jahr 2020 bereits 103 Millionen Smart Meter installiert, 88% davon im Privatsektor. Für Angreifende entstehen dadurch **hunderte Millionen potenzielle Einstiegspunkte in lokale wie nationale Stromnetze**. Insbesondere der Umstand, dass Smart Meter in leicht zugänglichen Umgebungen wie Häusern und öffentlichen Infrastrukturen installiert werden, erschwert es Energieunternehmen, ihre Infrastrukturgrenzen durchgehend zu überwachen sowie vor unbefugten Zugriffen und Datenmanipulation zu schützen. Diese neue Risikoexposition entsteht nicht zuletzt durch die grund-

legende AMI-Architektur. Nicht nur sind Millionen von Smart Metern eng miteinander und mit übergeordneten Systemen wie Home Energy Management Systems (HEMS) und Datenkollektoren vernetzt. Sie speichern zudem sensible Informationen über die Kommunikation im Smart Grid. Beides verstärkt das Risiko der **Gefahrenausbreitung, lateralen Bewegungen in der Infrastruktur und von Spillover-Effekten** in die Netzleit- und Fernwirktechnik der Kritischen Infrastruktur. Energieunternehmen und Stadtwerke haben in der Vergangenheit strategisch in die IT-Sicherheit investiert. Angreifende orientieren sich nun an dem nächsten schwächsten Glied – der AMI-Infrastruktur und den industriellen Komponenten. Diese benötigen **sofortige Systemhärtung, um die Cyberresilienz sicherzustellen**.



»Professionelle Cyberangriffe auf Advanced Metering-Infrastrukturen sind eine eindeutige und bestehende Gefahr. Das verheerendste Szenario ist ein Computerwurm, der sich in Advanced Metering-Infrastrukturen einschleicht und Millionen von Smart Metern dauerhaft außer Betrieb setzt«

Aaran Hanson et al. im »International Journal of Critical Infrastructure Protection«, 2017

## Cybersicherheit bis zur Edge schaffen

Rhebo schützt mit seinen Lösungen und Services seit fast zehn Jahren die Netzleittechnik und Fernwirktechnik von Energieunternehmen vor Cyberangriffen – von der Zentrale bis zu den Umspannwerken und Erneuerbare Energieanlagen. Mit Rhebo AMI Security erweitert Rhebo **den industriellen Cybersicherheits-Schutzschild von Energieerzeugern und -versorgern bis an die äußersten Grenzen** der Kritischen Infrastruktur. Rhebo AMI Security überwacht alle Kommunikationsvorgänge der Smart Meter, Datenkollektoren und HES auf Abweichungen von der zu erwartenden Kommunikation.

Angriffsaktivitäten wie laterale Bewegungen und Scans, Schadsoftware und Datenmanipulation aber auch technische Fehlerzustände werden **in Echtzeit erkannt und gemeldet**. Rhebo übernimmt den Betrieb des AMI-Monitoring und der integrierten Threat & Intrusion Detection. Unsere Expert:innen verfolgen die Anomalie-meldungen, prüfen die Kritikalität und schlagen Gegenmaßnahmen vor. **Energieversorgungsunternehmen können sich so auf ihre Kernaufgaben konzentrieren**, ohne die Sicherheit ihrer AMI aus den Augen zu verlieren.

# Einfach & Effektiv

## 3 Schritte zur sicheren Advanced Metering Infrastructure

1



Der erste einfache Schritt zu umfassender AMI-Sicherheit:

**Rhebo Industrial Security Assessment**

### Cybersicherheit beginnt mit Sichtbarkeit.

Das **Rhebo Industrial Security Assessment** für AMI liefert ein detailliertes Verständnis der AMI-Geräte, der Netzwerk- und Kommunikationsstruktur sowie bestehender Sicherheitsrisiken. Unsere Kunden erhalten eine umfassende Übersicht und klare, effektive Handlungsempfehlungen, um die Systemhärtung zu steigern.

### Sie profitieren von

- der Identifikation aller Geräte und Systeme in der AMI 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 AMI-Sicherheit:

**Rhebo Industrial Protector**

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

**Rhebo Industrial Protector** schafft mit kontinuierlichem Monitoring und integrierter Anomalieerkennung dedizierte industrielle Cybersicherheit in der AMI entsprechend des IT-SiG 2.0 und internationaler Standards. Es erweitert die bestehende Absicherung durch Firewalls um eine ganzheitliche, industrielle Angriffserkennung, indem es die Kommunikation zwischen Smart Metern, Datenkollektoren und dem Head End System überwacht und jegliche Anomalien in Echtzeit meldet.

### Sie profitieren von

- der Echtzeit-Sichtbarkeit des Kommunikationsverhaltens aller AMI-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**

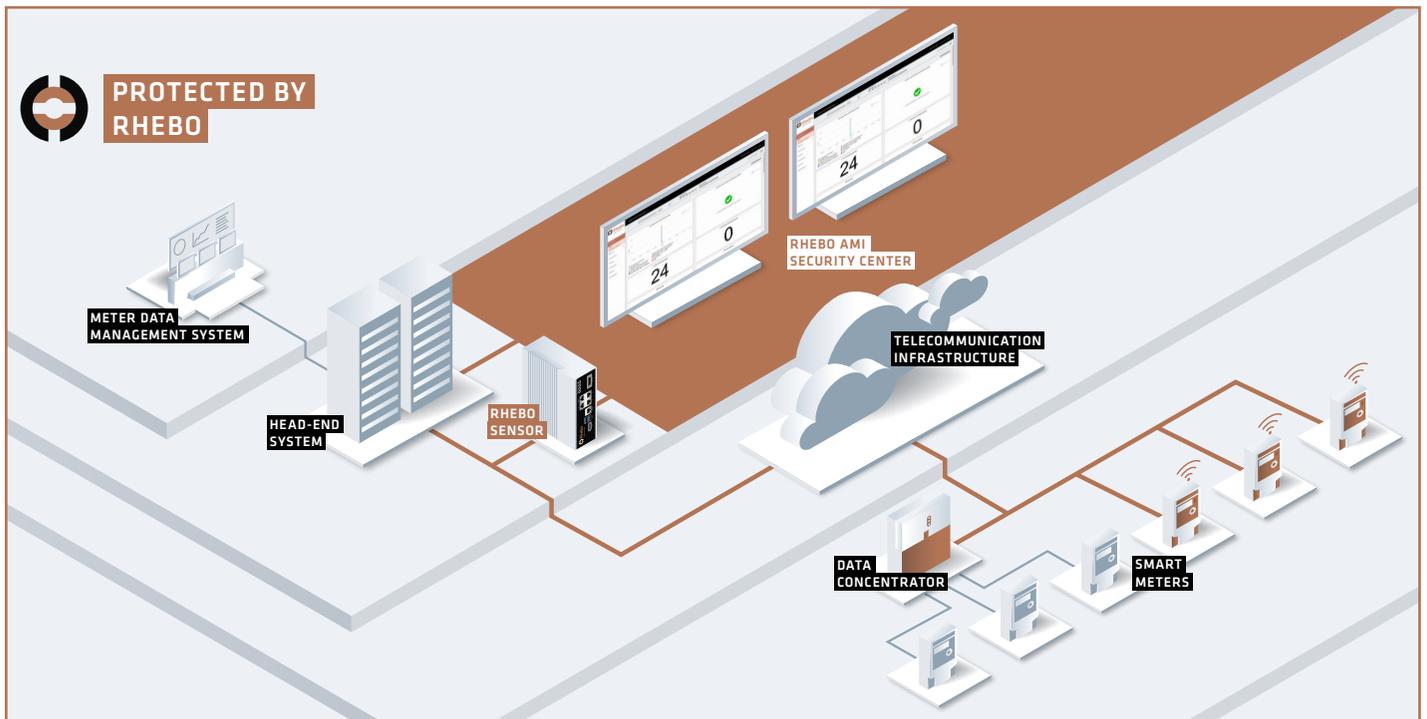
### AMI-Sicherheit braucht Ressourcen und Know-How.

Rhebo unterstützt Sie mit **Rhebo Managed Protection** beim Betrieb des AMI-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 AMI-Sicherheitsmonitorings;
- der schnellen forensischen Analyse und Aufklärung von AMI-Anomalien;
- der schnellen Handlungsfähigkeit bei Vorfällen;
- regelmäßigen AMI-Risikoanalysen für die kontinuierliche Verbesserung des Reifegrads Ihrer Cybersicherheit.

# Beispiel-Deployment von Rhebo AMI Security in der Advanced Metering Infrastructure



## Lesen schafft Wissen durch Rhebo AMI Security kontinuierlich analysierte Protokolle\*

ABB Redundant Network Routing Protocol	ESET Remote Administrator	Internet Printing Protocol	MRP	Remote Desktop Protocol	Stream Control Transmission Protocol
Acronis Backup	EtherCAT	Internet Small Computer Systems Interface	Munin Data Exchange Protocol	Remote Shell	Symantec Endpoint Protection Manager
Adobe Server	FTP Control	Inter-Switch Message Protocol	MySQL Client-Server Protocol	RK 512	Syslog
ARP	FTP Data	IPsec Authentication Header	Nagios	Routing Information Protocol	TCP Keep-Alive
AXIS Camera-Management	General Electric	IPsec Encapsulating Security Payload	NetBIOS	S7/S7+	TDS
BACnet	General Inter-ORB Protocol	IPv6	NFS	SentinelSRM	Telnet
Boot Service Discovery Protocol	GigE Vision Control Protocol	Java Remote Method Invocation	NTP	Sercos III	TFTP
Canon BJNP	GigE Vision Streaming Protocol	Kerberos	Omicron OMFind	Siemens Spectrum Power TG	Tivoli Storage Manager
CIP	Haag Damon	Landis+Gyr Outside Data Exchange Protocol	ONVIF Simple Object Access Protocol	Siemens SICAM PAS/PQS	TNS
Cisco	HART	Line Printer Daemon Protocol (LPD)	OpenProtocol	Simple Object Access Protocol	Undo License Manager
Cisco CDP	HP	Link Aggregation Control Protocol	Operation, Administration, Maintenance	Sinec H1	Veritas Backup Exec Client
Cisco CGMP	HP DTC	Link Aggregation Marker Protocol	OSPF	SKINNY	VMWare-Lab-Manager
Cisco DCE	HP Extended LLC	LDAP	PIM	Slow Protocol	VMware Server Console VNC
Cisco DTP	HP PROBE	LLC	Powerlink	SMA	VRRP
Cisco EIGRP	HSR	LLDP	Proficiency iFix	SMB	Web-Based Enterprise Management
Cisco WLCCP	HSRP	LLMNR	Profinet	SMTP	Web Services Discovery
Codesys	HTTP/S	LonTalk	Profinet-IO CM	SNMP	WinCC
COTP	iba Device Configuration Protocol	McAfee ePO	PSI	SqlNet2	X11
DCE/RPC	ICMP	mDNS	PTP	SQL Server Resolution Protocol	.NET TCP Binary Protocol
DECnet	IEC60870-5-104	Modbus	QNIX Qnet	SSDP	
DHCP	IEC61850-GOOSE	MQTT	QUIC	SSH	
DLMS/Cosem**	IEC61850-GSSE		Realtek Remote Control Protocol	SSL	
DNP3	IEC61850-MMS		Real Time Streaming Protocol	STOMP	
DNS	IEC61850-SMV			STP	
EAP over LA	IGMP				
ECTP	Intel Advanced-Network-Services				
EGP					
ELCOM-90					

hervorgehobene Einträge:  
industriespezifische Protokolle

\* Stand September 2022  
\*\* verfügbar ab Januar 2023

# Rhebo OT Security Made Simple



## LANGJÄHRIGE ERFAHRUNG

in industriellen Sicherheitslösungen für Energie- und Wasserunternehmen.



## DEDIZIERTE UND EINFACHE LÖSUNG

für die kosteneffiziente Integration in die Operational Technology, Advanced Metering Infrastructure und IIoT.



## UMFASSENDE UNTERSTÜTZUNG

bei der schnellen und gezielten Steigerung der industriellen Cyberresilienz.



## AMI SECURITY MADE SIMPLE

durch OT-fokussierte Sicherheitsanalyse und intelligente Visualisierung, ohne in die AMI eingreifen zu müssen.



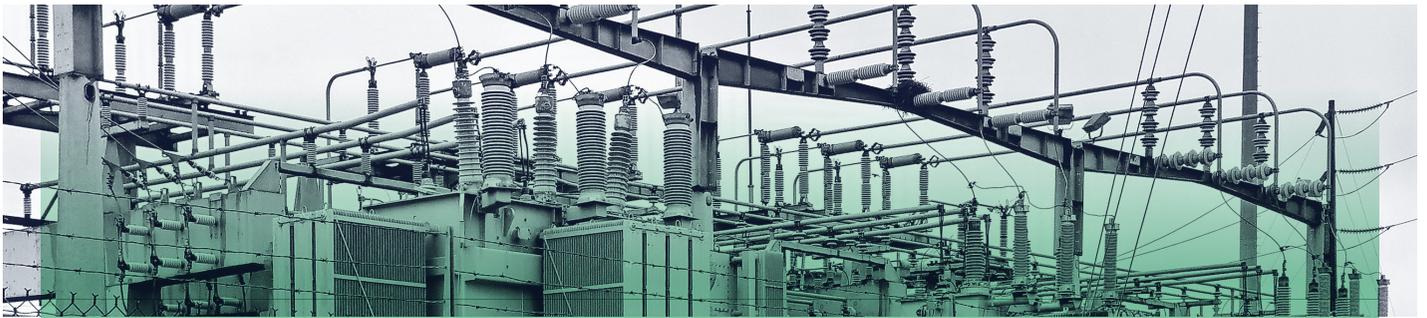
## SICHERHEIT VOR BEKANNTEN UND NEUARTIGEN CYBERANGRIFFEN

durch Monitoring, Asset Discovery und Angriffserkennung sowie Event-Korrelation von HES, Netzwerk und Smart Metern.



## ENDE-ZU-ENDE-SICHERHEIT

durch Anomalieerkennung zur Vermeidung der Gefahrenausbreitung über die OT, IIoT und Advanced Metering Infrastructure.



»Mit Rhebo können wir sichergehen, dass wir jede Auffälligkeit in unserer Netzleittechnik in Echtzeit gemeldet bekommen und umgehend reagieren können«.

Dirk Hollmach | Leiter Netzführung | Mitnetz Strom



## SICHERHEIT VOR BESTEHENDEN SCHWACHSTELLEN

durch regelmäßige AMI-Risikobewertungen, -Sicherheitsanalysen und -Reifegradbeurteilungen.



## SICHERSTELLUNG DER HANDLUNGSFÄHIGKEIT

durch Rhebo Expert:innen-Unterstützung bei Risikoanalyse, Betrieb und forensischer Analyse.



## SYSTEMSICHERHEIT

durch flexible und kosteneffiziente Integration der Rhebo-Lösung auf IIoT-Geräten und Netzwerkkomponenten.



## SICHERHEIT VOR INTRANSPARENTEN KOSTEN

durch einfache Lizenzpakete und unkomplizierte Lösungsintegration.



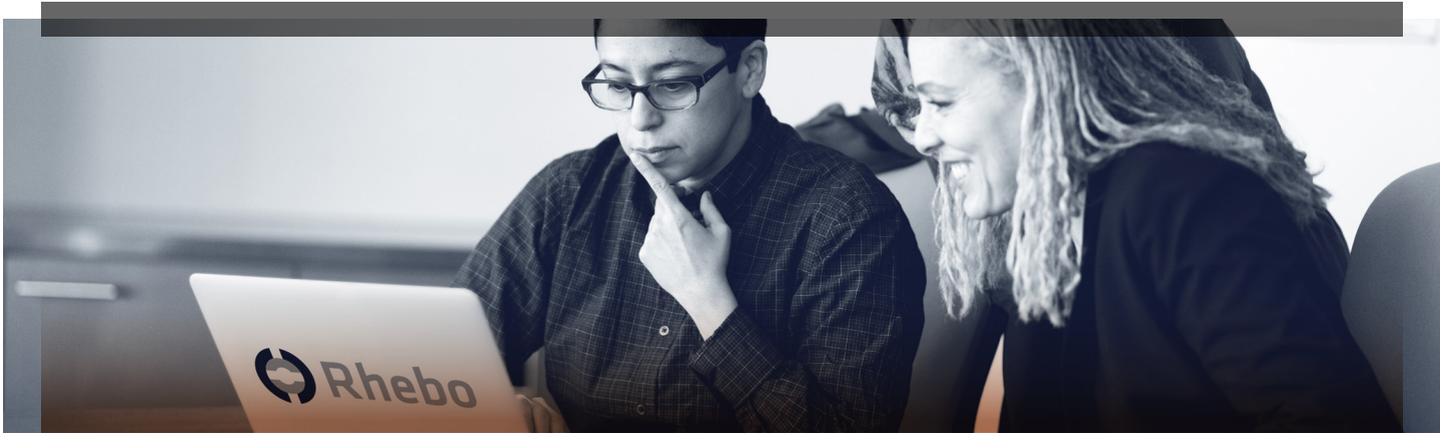
## COMPLIANCE SICHERSTELLEN

durch System zur Angriffserkennung für die OT nach ITSiG 2.0 und einschlägigen Sicherheitsstandards.



## VERTRAUENSVOLLE SICHERHEIT MADE IN GERMANY

nach den Anforderungen der European Cyber Security Organisation (ECSO) und DSGVO.



## Machen Sie Ihre AMI-Netzwerk-Risikoanalyse oder buchen Sie eine Demo

[www.rhebo.com](http://www.rhebo.com) | [sales@rhebo.com](mailto:sales@rhebo.com) | +49 341 3937900

### Entdecken Sie industrielle End-to-End-Cybersicherheit von Rhebo

➤ [Rhebo OT Security](#)

➤ [Rhebo IIoT Security](#)

### Geschützt durch Rhebo



### OT Sicherheit Made In Germany



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