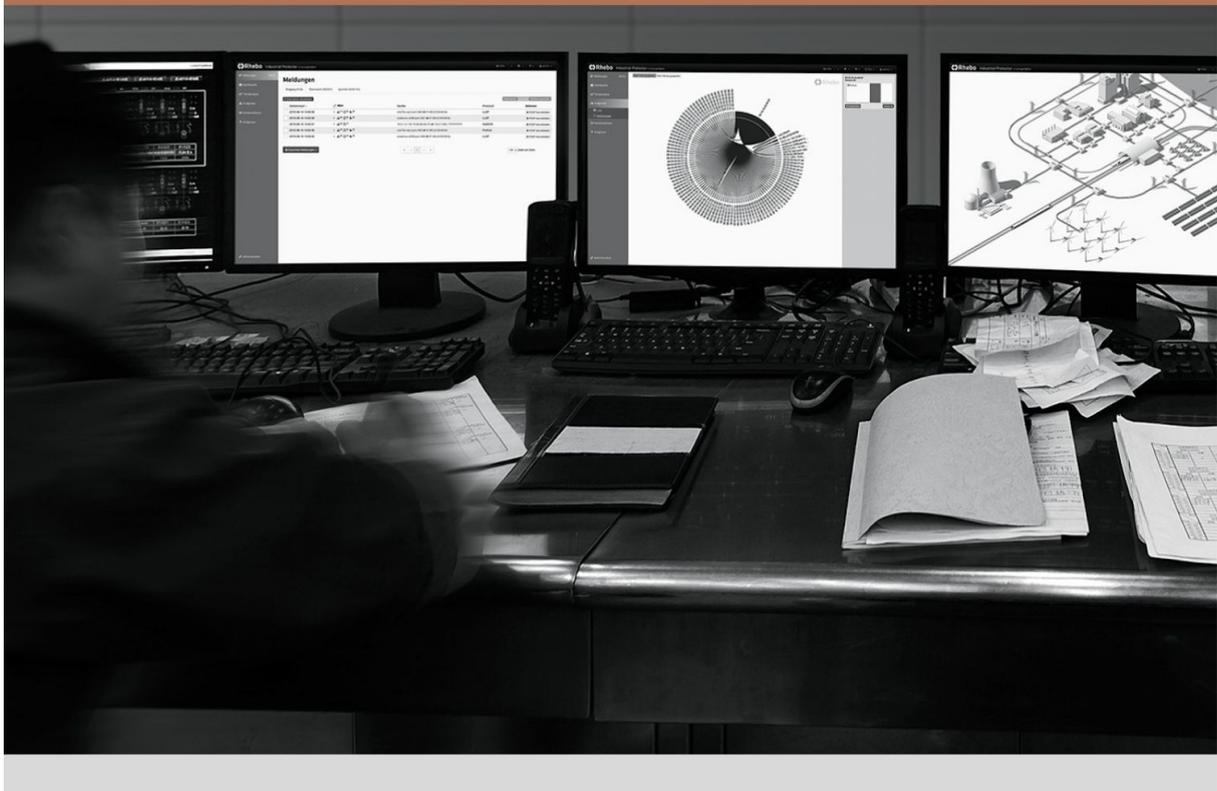


# Rhebo RISSA QuickCheck Anomalie-Report Ergebnisse

RISSA-QuickCheck-Analyse vom 01.02.2019

Zur Verfügung gestellt von RHEBO für Customer AG



## Inhaltsverzeichnis

<b>Hinweise und Legende</b>	<b>2</b>
<b>Datenbasis</b>	<b>3</b>
Erfassungszeitraum	3
Datensatz	3
<b>Übersicht</b>	<b>4</b>
Zusammenfassung	4
Geräte	4
Hersteller (Auszug)	5
Protokolle (Auszug)	5
Anomalien	5
<b>Ausgewählte Ergebnisse</b>	<b>6</b>
Öffentliche IP-Adresse	6
Verwundbare Firmware	6
Weitere Anomalien mit hohem Risiko	7
Unsicherer Login	7
Zyklische Nachricht zu spät	7
TCP-Fenster mit Größe 0	8
Weitere Anomalien mit mittlerem Risiko	8
Subnetz nicht einsehbar	9
<b>Nächste Schritte</b>	<b>10</b>

## Hinweise und Legende

Dieses Dokument nutzt die folgenden Bewertungen:

-  Hohes Risiko für Stabilität bzw. Sicherheit des Netzwerks, bedarf sofortiger Behebung.
-  Warnung vor Bedrohung oder erhöhtem Risiko. Ggf. weitere Untersuchungen notwendig.
-  Keine ernststen Bedrohungen vorgefunden. Weiterführendes Monitoring wird empfohlen.
-  Keine Wertung möglich. Unvollständige Daten oder Analyse aus anderen Gründen nicht durchführbar.

## Datenbasis

### Erfassungszeitraum

Die Aufzeichnungen betreffen Daten, die zwischen dem 07.06.2018 um 10:58 Uhr und dem 26.06.2018 um 17:47 Uhr erhoben wurden.

**From**



Thu, Jun 7, 2018 10:58 AM

**To**



Tue, Jun 26, 2018 5:47 PM

**Range**



19 d 6 h 49 min 31 s



### Datensatz

Zur Verfügung gestellt wurden 3 PCAP-Dateien, die in diesem Zeitraum aufgezeichnet wurden:

- anlage\_001.pcap (104 MB)
- anlage\_002.pcap (97 MB)
- uplink\_a.pcap (30 MB)

Die Aufzeichnungen umfassen insgesamt ca. 231 MB.

# Übersicht

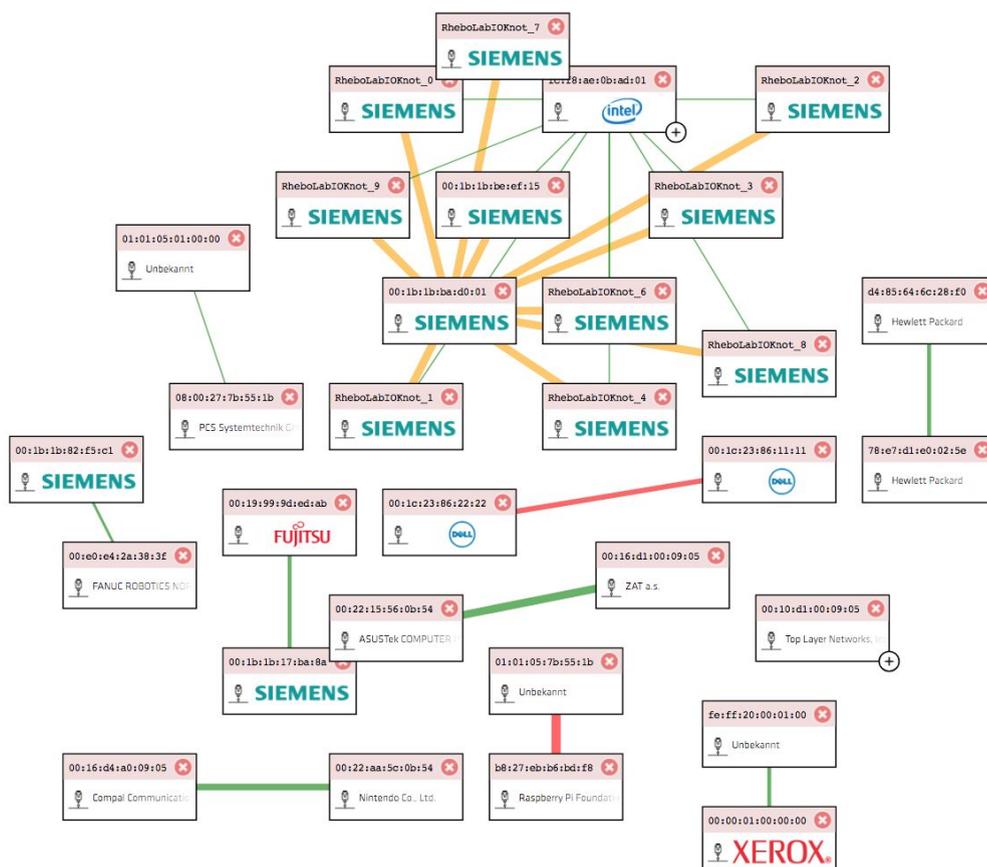
## Zusammenfassung

Die Stabilität des Netzwerks wird insgesamt mit 8.0 von 10 bewertet und liegt damit leicht über dem Durchschnitt vergleichbarer Netzwerke.

Die Sicherheit des Netzwerks wird mit 4.6 von 10.0 bewertet und liegt damit deutlich unter dem Durchschnitt vergleichbarer Netzwerke.

## Geräte

Rhebo Industrial Protector zeigt im analysierten Netzwerk 31 Geräte in 10 Clustern an. In Cluster A wird vor allem mittels der Protokolle Profinet und S7 kommuniziert. Die weiteren Cluster bilden dagegen ein typisches IT-Netzwerk, in dem vor allem per HTTP, SMB und LDAP kommuniziert wird.



Während in den meisten Clustern nur wenige Probleme identifiziert wurden, scheint Cluster A vielfach unter überlasteter Netzwerkinfrastruktur zu leiden. Hier finden sich viele Anomalien der Typen “Zyklische Nachricht zu spät” sowie “IP-Header-Fehler”.

Die Sicherheit des Netzwerks scheint bedroht zu sein. Es findet Kommunikation mit dem Internet statt. Es wurden außerdem Hinweise darauf gefunden, dass einige Geräte von Schadsoftware befallen sind. Darüber hinaus wird offensichtlich verwundbare Firmware verwendet.

### Hersteller (Auszug)

Hersteller	Anzahl
Siemens	13
Hewlett Packard	2
Dell	1
Intel	1
Fujitsu	1

### Protokolle (Auszug)

Protokoll	Datenvolumen	Pakete
Profinet	191 MB	170.430
S7	23 MB	41.051
HTTP	7 MB	6.534
SMB	5 MB	4.991
LDAP	1 MB	1.337

### Anomalien

Typ	Anzahl
Zyklische Nachricht zu spät	571
IP-Header-Fehler	137
Öffentliche IP-Adresse	23

Unsicherer Login	5
TCP-Fenster mit Größe 0	4
<b>Weitere Anomalien</b>	<b>274</b>

## Ausgewählte Ergebnisse

Im Folgenden sind ausgewählte Ergebnisse der mittels Rhebo Industrial Protector durchgeführten Kurzanalyse aufgeführt. Wenn Sie eine detaillierte Analyse aller Anomalien in Ihrem Steuerungsnetz mit Risikobewertung und Handlungsempfehlungen wünschen, empfehlen wir die Durchführung eines vollständigen Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudits. Informieren Sie sich unter <https://rhebo.com/de/service/rissa-rhebo-industrie-4-0-stabilitaets-und-sicherheitsaudit/>.

### Öffentliche IP-Adresse

Etliche Hosts versuchen regelmäßig, mit Servern im öffentlichen Internet zu kommunizieren. Darunter finden sich vor allem versuchte Software-Updates, die aber offenbar von einer Firewall blockiert werden. In einem Fall wurde allerdings der Host "6f7cc0217ae.dyn.rostelecom.ru" kontaktiert. Es wurden erfolgreich ca. 7 kB an Daten ausgetauscht. Diese Kommunikation erfolgte verschlüsselt. Es ist nicht davon auszugehen, dass es sich hier um erwünschte Kommunikation handelt.

Erstes Auftreten	Wert	Endgeräte	Protokoll
2019-02-04 10:36:02	 (2)	<a href="#">145.254.160.237 / 00:00:01:00:00:00</a> ⇌ <a href="#">65.208.228.223 / fe:ff:20:00:01:00</a>	HTTP
  Öffentliche IP-Adresse: 145.254.160.237			
  Öffentliche IP-Adresse: 65.208.228.223			

**Es gibt 2 weitere Fälle von Kommunikation mit öffentlichen IP-Adressen in Ihrem Netzwerk.**

### Verwundbare Firmware

Der Host "switch-a-003" läuft mit der Firmwareversion 5.1.0. Für diese bestehen mehrere Sicherheitslücken, die es einem lokalen Angreifer erlauben, beliebigen Code auf dem System auszuführen. Die Firmware sollte daher dringend aktualisiert werden.

<b>CVE</b> CVE-2013-3633	<b>Schwere</b> <b>Hoch</b>
<b>Angriffswert</b> 8	<b>Gewichtung</b> 8.5
<b>Beschreibung</b> The web interface on Siemens Scalance X200 IRT switches with firmware before X-200IRT 5.1.0 relies on client-side privilege checks, which allows remote authenticated users to execute arbitrary commands via unspecified vectors.	

**Es gibt 3 weitere Fälle von verwundbarer Software in Ihrem Netzwerk.**

### Weitere Anomalien mit hohem Risiko

<input type="checkbox"/> Erstes Auftreten	 Wert	Endgeräte	Protokoll
<input type="checkbox"/> 2019-02-04 15:33:26	 (1)	<a href="#">10.0.0.130 / f8:db:88:74:ca:a4</a> ⇌ <a href="#">10.0.0.66 / b8:27:eb:b6:bd:f8</a>	<a href="#">CUSTOM: TCP Port = 445</a>
<b>IP-Adresse: 10.0.0.130</b> Nachricht: Address-Scan			
<input type="checkbox"/> 2019-02-04 15:33:09	 (1)	<a href="#">10.0.0.66 / b8:27:eb:b6:bd:f8</a> ⇌ <a href="#">10.0.0.130 / f8:db:88:74:ca:a4</a>	<a href="#">FTP Control</a>
<b>IP-Adresse: 10.0.0.130</b> Nachricht: Fehlgeschlagener Anmeldeversuch			
<input type="checkbox"/> 2019-02-04 15:33:08	 (1)	<a href="#">10.0.0.101 / f8:db:88:4d:a2:fe</a> ⇌ <a href="#">10.0.0.130 / f8:db:88:74:ca:a4</a>	<a href="#">FTP Control</a>
<b>IP-Adresse: 10.0.0.101</b> Nachricht: Klartext-Passwort			

**Es wurden insgesamt 13 weitere Anomalien mit hohem Risiko in Ihrem Netzwerk gefunden. Davon betroffen sind 7 Endgeräte.**

### Unsicherer Login

Die Anmeldung am SMB-Server "fileserv-002" erfolgt via NT Lan Manager. Diese Authentifizierungsmethode ist als veraltet anzusehen. Ein lokaler Angreifer im Netzwerk wäre unter Umständen in der Lage, Anmeldedaten inklusive der Passwörter einzusehen. Ein Umstieg auf eine zeitgemäße Alternative wie Kerberos wird empfohlen.

**Es gibt 3 weitere Fälle von unsicheren Login-Methoden in Ihrem Netzwerk.**

### Zyklische Nachricht zu spät

Der Host "sps-015" sendet am 11.06.2018 zwischen 04:31 Uhr und 07:01 Uhr mehrfach zyklische Nachrichten, die außerhalb der Taktfrequenz liegen und damit zu spät ankommen. Es handelt sich um Kommunikation mit den Hosts "sps-027" und "sps-051" unter Nutzung des Protokolls Profinet. Ein Grund hierfür kann überlastetes Netzwerkequipment sein, wie zum Beispiel Switches, Router oder auch Kabel.

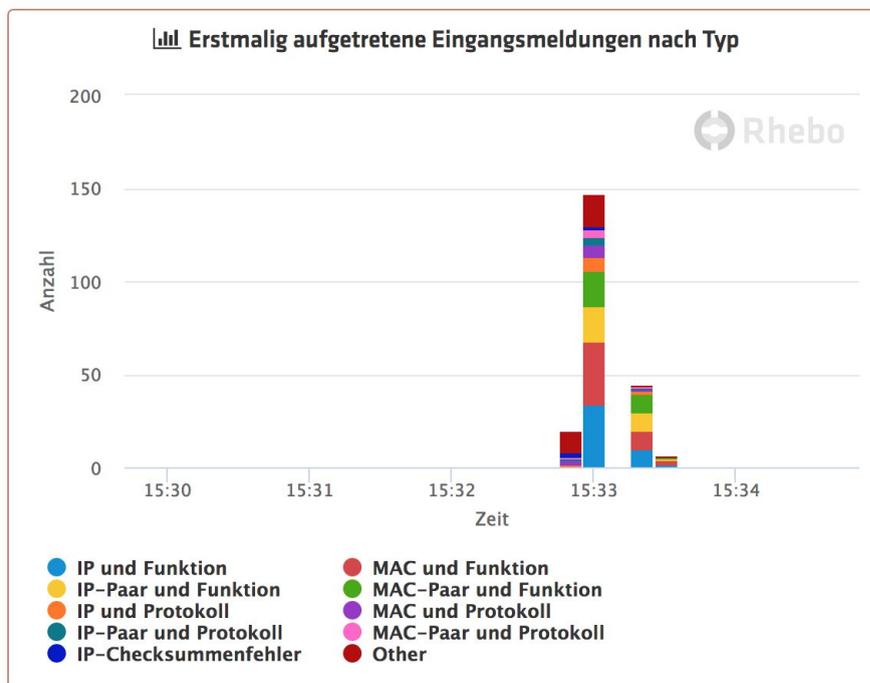
**Es gibt 7 weitere Hosts mit dieser Auffälligkeit in Ihrem Netzwerk.**

### — TCP-Fenster mit Größe 0

Der Host "leitstelle-071" meldet am 08.06.2018 zwischen 11:23 Uhr und 11:43 Uhr mehrfach ein TCP-Fenster mit einer Größe von 0. Es handelt sich um Kommunikation mit dem Host "fernwartung-409" unter Nutzung des Protokolls HTTP. Diese Meldung bedeutet, dass das jeweilige Gerät zu diesem Zeitpunkt keine Daten auf der entsprechenden TCP-Verbindung empfangen kann. Ein Grund hierfür kann sein, dass das Gerät überlastet ist oder die jeweilige Anwendung zum Beispiel in einer Endlosschleife hängt.

**Es gibt 2 weitere Hosts mit dieser Auffälligkeit in Ihrem Netzwerk.**

### — Weitere Anomalien mit mittlerem Risiko



**Es wurden insgesamt 31 weitere Anomalien mit mittlerem Risiko in Ihrem Netzwerk gefunden. Davon betroffen sind 11 Endgeräte.**



## Subnetz nicht einsehbar

Mehrere Hosts aus dem Subnetz 10.71.2.0/24 senden offenbar fehlerhafte TCP-Pakete in die Netze 10.71.3.0/24 sowie 10.71.55.0/24. Für eine genauere Analyse ist es ratsam, den dort auftretenden Verkehr mitzuschneiden. Dies kann zum Beispiel im Rahmen eines umfassenden [Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudits](#) geschehen.

## Ihre nächsten Schritte

Mit dem RISSA QuickCheck haben Sie sich einen ersten Überblick zum Status Ihres Steuerungsnetzes verschafft. Die Momentaufnahme Ihrer Steuerungskommunikation zeigt bereits das Optimierungspotential für eine Verbesserung der Netzwerksicherheit und Effizienz. Mit den nächsten Schritten können Sie Ihr Verständnis der Gefährdungsvektoren weiter ausbauen und die Basis für lückenlose Transparenz und Vorfallerkennung schaffen.

Das sind unsere Empfehlungen für Sie:

- 1. Detailanalyse zu allen Anomalien und vollständiges Asset Inventory erhalten:**  
Bei einem [Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit](#) analysieren wir Ihre Steuerungskommunikation über alle Netze und Subnetze über einen Zeitraum von 7-14 Tagen. Sie erhalten:
  - Klarheit über alle im Steuerungsnetz aktiven Assets, Kommunikationsverbindungen und -vorgänge,
  - Details zu allen verdächtigen Vorgängen, die auf Sicherheitsrisiken oder technische Fehlerzustände hinweisen (Bericht),
  - weiterführende Handlungsempfehlung zu allen identifizierten Anomalien (1-Tages-Workshop).
- 2. Kontinuierliche Überwachung und Echtzeit-Anomalieerkennung:**  
Integrieren Sie [Rhebo Industrial Protector](#) als kontinuierliches Network Condition Monitoring in Ihr Steuerungsnetz. Damit wissen Sie jederzeit in Echtzeit:
  - ob Ihr Steuerungsnetz langfristig stabil und sicher funktioniert.
  - ob verdächtige Vorgänge die Sicherheit, Anlagenverfügbarkeit oder Prozessstabilität gefährden.
  - alle Details zu einem Vorfall für die forensische Analyse und Weiterleitung an intern Verantwortliche und Behörden

Sie können Rhebo Industrial Protector auch im Blackbox-Modus einsetzen, um ausschließlich für rückblickende forensische Analysen alle Daten sichern.

- 3. Anomalien einschätzen und Cybersicherheit und Verfügbarkeit effektiv verbessern:**  
Mit dem ReadyNow Service von Rhebo unterstützen wir Sie auf Wunsch auch umfassend bei der Einschätzung von Anomalien und der Evaluation geeigneter Maßnahmen. Je nach Service-Level führen wir regelmäßige Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudits durch. Bitte sprechen Sie uns zum Rhebo ReadyNow Service direkt an.

# Ihre weiterführenden Informationen

<h2>Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit</h2>	<h2>Rhebo Industrial Protector für Industrie 4.0</h2>	<h2>Rhebo Industrie 4.0 für Kritische Infrastrukturen</h2>
 <p><b>RISSA Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit im Steuerungsnetz</b></p> <p>Kritische Infrastrukturen und automatische Fertigungsanlagen stellen zunehmend mit Individualität, Komplexität und Skalierbarkeit die Herausforderung dar. Die Vernetzung der industriellen Steuerungsnetze mit SCADA, MES und ERP-Systemen bringt große Chancen in der Produktion und ermöglicht vollständige Prozess- und Anlagenüberwachung.</p> <p>Mit der Vernetzung ergeben sich neue Risiken im Bereich Stabilität und Cybersecurity. Zudem erhöht die Komplexität der vernetzten Steuerungsnetze die Möglichkeit für Fehlerzustände, Probleme im Datenverkehr und Kapazitätsengpässe.</p> <p><b>Vollständige Stabilitäts- und Sicherheitsanalyse</b></p> <p>RISSA - Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit ist eine schnelle und vollständige Stabilitäts- und Sicherheitsanalyse industrieller Steuerungsnetze. Rhebo Industrial Protector ist das zentrale Werkzeug für die Analyse und die Identifizierung von Schwachstellen und deren Auswirkungen. Es ermöglicht eine vollständige Analyse der Produktions- und Steuerungsnetze für Produktionsanlagen und kritische Infrastrukturen.</p> <p><b>Workshop mit priorisierten Handlungsempfehlungen</b></p> <p>In einem Workshop am Ende des Audits werden alle Ergebnisse in einer Zusammenfassung zusammengefasst. Diese Zusammenfassung enthält eine detaillierte Liste aller Schwachstellen und deren Auswirkungen. Sie enthält auch eine Liste von Handlungsempfehlungen zur Beseitigung der Schwachstellen und zur Verbesserung der Stabilität und Sicherheit des Steuerungsnetzes.</p> <p><b>WORKSHOP UND REPORT ERHALTEN</b></p> <ul style="list-style-type: none"> <li>Detaillierte Liste aller Schwachstellen und deren Auswirkungen</li> <li>Detaillierte Liste aller Schwachstellen und deren Auswirkungen</li> <li>Ausgaben zur Qualität des Netzwerks in Bezug auf die spezifischen Anforderungen des industriellen Steuerungsnetzes (z. B. Echtzeitkommunikation, Redundanz, Skalierbarkeit)</li> <li>Vorschläge für kontinuierliche Verbesserungsmaßnahmen von Stabilität und Cybersecurity</li> <li>Prüfung von Handlungsempfehlungen zur Beseitigung von Schwachstellen und Beseitigung von Fehlerrisikofaktoren</li> </ul> <p><b>RISSA REPORT</b></p> <ul style="list-style-type: none"> <li>Online-Analyse</li> <li>Umfassende Datenanalyse</li> </ul> <p><b>THE MESSAGE BLITZ</b></p> <ul style="list-style-type: none"> <li>Digitale Transparenz über vollständige Datenanalyse und Identifizierung von Schwachstellen, Konfigurationsänderungen und vollständigen Prozessen</li> <li>Tag- und Nacht-Erfassung der industriellen Cybersecurity</li> <li>Selbständige Erkennung von Schwachstellen, Konfigurationsänderungen und vollständigen Prozessen</li> <li>Einfache Fortführung des Monitorings zur kontinuierlichen Verbesserung von Stabilität und Cybersecurity</li> <li>Hohe Compliance bei den geringsten Kundeninvestitionen</li> </ul> <p><b>HERAUSFORDERUNGEN DES INDUSTRIAL INTERNET OF THINGS (IIOT) BELEGEN</b></p> <ul style="list-style-type: none"> <li>Anlagenfehler vermeiden</li> <li>Komplexität überwinden</li> <li>Effektivität schnell steigern</li> <li>Skalierbarkeit sicherstellen</li> <li>Benutzerfreundlichkeit gewährleisten</li> <li>Cloud- und Edge-Integration</li> <li>Sicherheitsrisiken vermeiden</li> </ul> <p><b>GEWÄHREN PRODUKTIVE ERKENNEN &amp; PRODUKTIONSCÄPPEL VERMEIDEN</b></p> <ul style="list-style-type: none"> <li>ANLAGENVERFÜGBARKEIT ERHÖHEN &amp; SYSTEMFÄHIGKEIT STEIGERN</li> <li>NORMEN UND STANDARDS ERHALTEN</li> </ul>	 <p><b>Rhebo Industrial Protector in Industrie 4.0</b></p> <p>Rhebo Industrial Protector sichert Ihre Steuerungsnetze gegen betriebliche Störungen und Cyberangriffe – lückenlos und in Echtzeit.</p> <p><b>REIFERHEITSPUNKTE SOFORT VERMEIDEN</b></p> <p>Rhebo Industrial Protector misst und prognostiziert in Echtzeit jede Anomalie in der IT-Kommunikation, die zu Störungen oder Ausfällen der Fertigung führen kann. Einmalige oder wiederkehrende Anomalien werden sofort erkannt und gemeldet.</p> <p><b>CYBERANGRIFFE IN ECHTZEIT ERKENNEN</b></p> <p>Rhebo Industrial Protector erkennt Cyberangriffe, bevor sie vollendet sind. Er reagiert umgehend an den Angriffspunkten.</p> <p><b>GAS UND SYSTEMEFFIZIENZ STEIGERN</b></p> <p>Rhebo Industrial Protector unterstützt die systemübergreifende Datenintegration für die effektive Ansteuerung Ihrer Big Data Strategie.</p> <p><b>Industrial Control Systems stabil und effizient steuern</b></p> <p>Industrial Control Systems (ICS, deutsch Steuerungszentralen) sind in der Industrie 4.0 und dem industriellen Internet der Dinge (IIoT) das Herzstück einer hochproduktiven Fertigung. Sie sind jedoch auch das zentrale Element für die Produktion und die Fertigung. Die Komplexität der ICS ist durch die Vernetzung der Fertigungsanlagen mit dem industriellen Internet der Dinge (IIoT) und der Integration von Cloud- und Edge-Technologien weiter gewachsen. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung.</p> <p>Rhebo Industrial Protector <b>überwacht, analysiert und evaluiert die komplette Cybersecurity in Ihrer Steuerungszentrale</b>. Es ist ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung.</p> <p><b>HERAUSFORDERUNGEN DES INDUSTRIAL INTERNET OF THINGS (IIOT) BELEGEN</b></p> <ul style="list-style-type: none"> <li>Anlagenfehler vermeiden</li> <li>Komplexität überwinden</li> <li>Effektivität schnell steigern</li> <li>Skalierbarkeit sicherstellen</li> <li>Benutzerfreundlichkeit gewährleisten</li> <li>Cloud- und Edge-Integration</li> <li>Sicherheitsrisiken vermeiden</li> </ul> <p><b>GEWÄHREN PRODUKTIVE ERKENNEN &amp; PRODUKTIONSCÄPPEL VERMEIDEN</b></p> <ul style="list-style-type: none"> <li>ANLAGENVERFÜGBARKEIT ERHÖHEN &amp; SYSTEMFÄHIGKEIT STEIGERN</li> <li>NORMEN UND STANDARDS ERHALTEN</li> </ul>	 <p><b>Rhebo Industrial Protector in Kritischen Infrastrukturen</b></p> <p>Rhebo Industrial Protector sichert Fernwirklinien gegen Cyberbedrohungen und Störungen – lückenlos zu jeder Zeit und in Echtzeit.</p> <p><b>REIFERHEITSPUNKTE SOFORT VERMEIDEN</b></p> <p>Rhebo Industrial Protector misst und prognostiziert in Echtzeit jede Anomalie in der Datenkommunikation, die zu Störungen oder Ausfällen führen kann.</p> <p><b>DIGITALE COMPLIANCE SICH ERHALTEN</b></p> <p>Rhebo Industrial Protector analysiert Ihre Konformität und unterstützt Sie bei der Erfüllung der Anforderungen nach dem IT-Sicherheitsgesetz.</p> <p><b>SYSTEMEFFIZIENZ STEIGERN</b></p> <p>Rhebo Industrial Protector unterstützt die systemübergreifende Datenintegration für die effektive Ansteuerung Ihrer Big Data Strategie.</p> <p><b>Energie-, Gas- und Wasserwirtschaft zuverlässig und sicher betreiben</b></p> <p>Die Sicherheit der Versorgungsnetze liegt im effektiven Schutz der Fernwirknetze. Nur wenn in einem Prozess keine Operationen stattfinden, kann die Produktion gegen Cyberangriffe geschützt werden. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung.</p> <p>Rhebo Industrial Protector <b>überwacht, analysiert und evaluiert die komplette Cybersecurity in Ihrer Fernwirkzentrale</b>. Es ist ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung. Die ICS sind heute ein zentraler Bestandteil der Produktion und der Fertigung.</p> <p><b>HERAUSFORDERUNGEN DES INDUSTRIAL INTERNET OF THINGS (IIOT) BELEGEN</b></p> <ul style="list-style-type: none"> <li>Anlagenfehler vermeiden</li> <li>Komplexität überwinden</li> <li>Effektivität schnell steigern</li> <li>Skalierbarkeit sicherstellen</li> <li>Benutzerfreundlichkeit gewährleisten</li> <li>Cloud- und Edge-Integration</li> <li>Sicherheitsrisiken vermeiden</li> </ul> <p><b>GEWÄHREN PRODUKTIVE ERKENNEN &amp; PRODUKTIONSCÄPPEL VERMEIDEN</b></p> <ul style="list-style-type: none"> <li>ANLAGENVERFÜGBARKEIT ERHÖHEN &amp; SYSTEMFÄHIGKEIT STEIGERN</li> <li>NORMEN UND STANDARDS ERHALTEN</li> </ul>
<p><a href="#">Download Datenblatt</a></p>	<p><a href="#">Download Datenblatt</a></p>	<p><a href="#">Download Datenblatt</a></p>

# Wie sicher ist Ihr Industrial Control System?

Lassen Sie Ihr Netzwerk auf  
Herz und Nieren prüfen.

Kontaktieren Sie uns

[www.rhebo.com](http://www.rhebo.com) | [sales@rhebo.com](mailto:sales@rhebo.com) | +49 341 393790 202

## Über Rhebo

Rhebo ist ein deutsches Technologieunternehmen, das sich auf die Ausfallsicherheit industrieller Steuerungssysteme mittels Überwachung der Datenkommunikation spezialisiert hat. Rhebo bietet Hardware, Software und Dienstleistungen, um vernetzte industrielle Steuerungssysteme und Kritische Infrastrukturen zu schützen

und ihre Produktivität zu steigern. Rhebo ist einer der 30 Top-Anbieter für die industrielle Sicherheit in Gartner's »Marktführer für betriebstechnische Sicherheit 2017«. Das Unternehmen ist zudem Mitglied im Teletrust – Bundesverband IT-Sicherheit e.V.

