BayWa r.e.

Rhebo

Was passiert in Ihrem Windpark wenn niemand hinsieht?

IT-Sicherheit in der Praxis.

r.e.think energy

IT-Sicherheit in der Praxis

1. Was ist Anomalie-erkennung?
2. Aufbau und Besonderheiten
3. Erkentnisse
4. Fazit

Was ist Anomalieerkennung?

Was ist Anomalieerkennung?

Wie funktioniert Anomalieerkennung?

Monitoring & Dekodierung der Kommunikation, sowie Bestandsaufnahme aller Assets via Deep Packet Inspection

Automatisches Lernen der Kommunikationsmuster

Meldung aller Ereignisse (Anomalien), die zu Betriebsstörungen führen können

Was ist Anomalieerkennung?

Welchen Vorteil hat Anomalieerkennung im Netzwerk?

Kontinuierliches Netzwerkmonitoring schafft Transparenz in der Steuerungstechnik

Frühzeitige Erkennung von Angriffen und Störungen

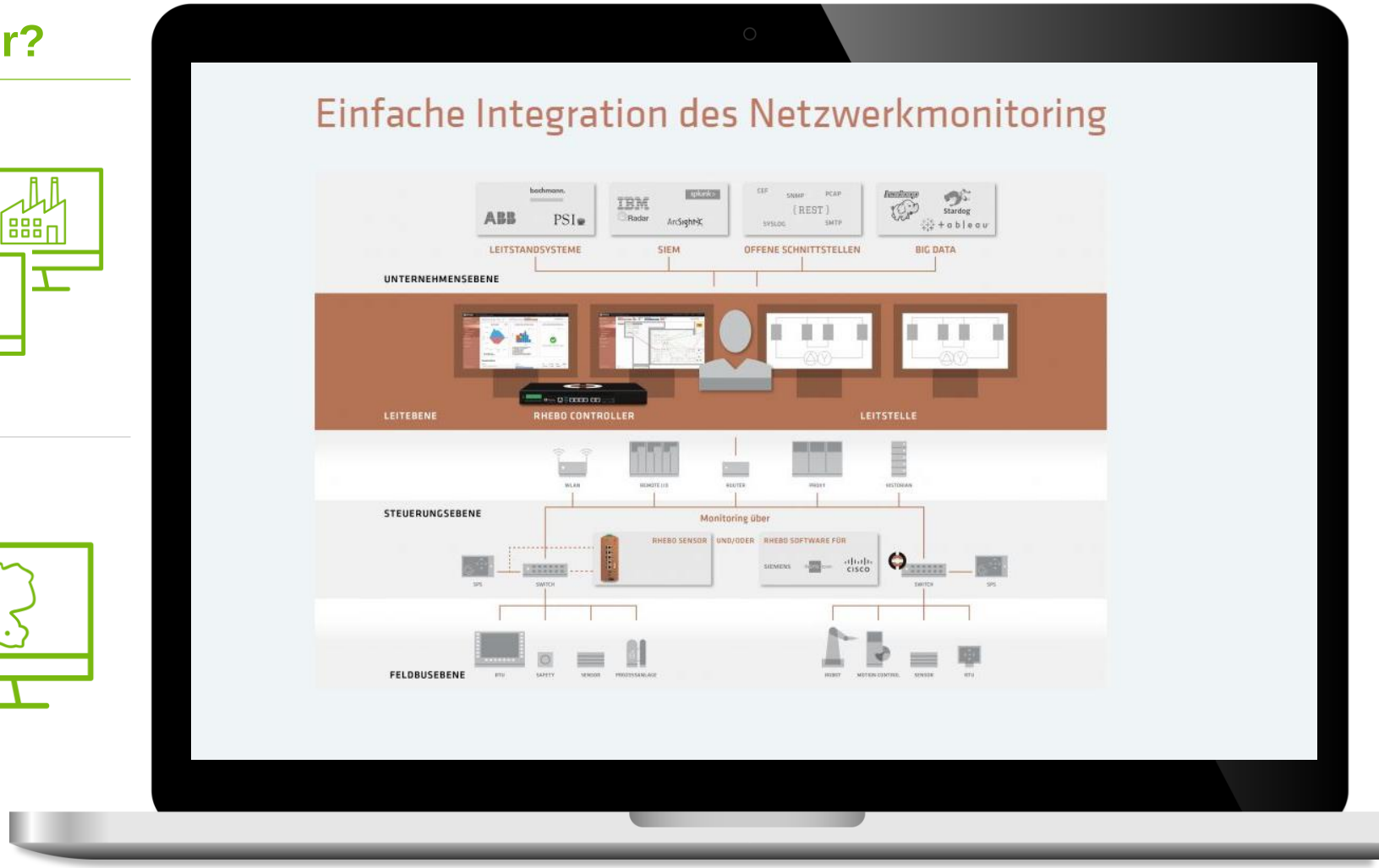
Stillstände können verhindert und die Verfügbarkeit erhöht werden

Was ist Anomalieerkennung?

Warum Rhebo Industrial Protector?

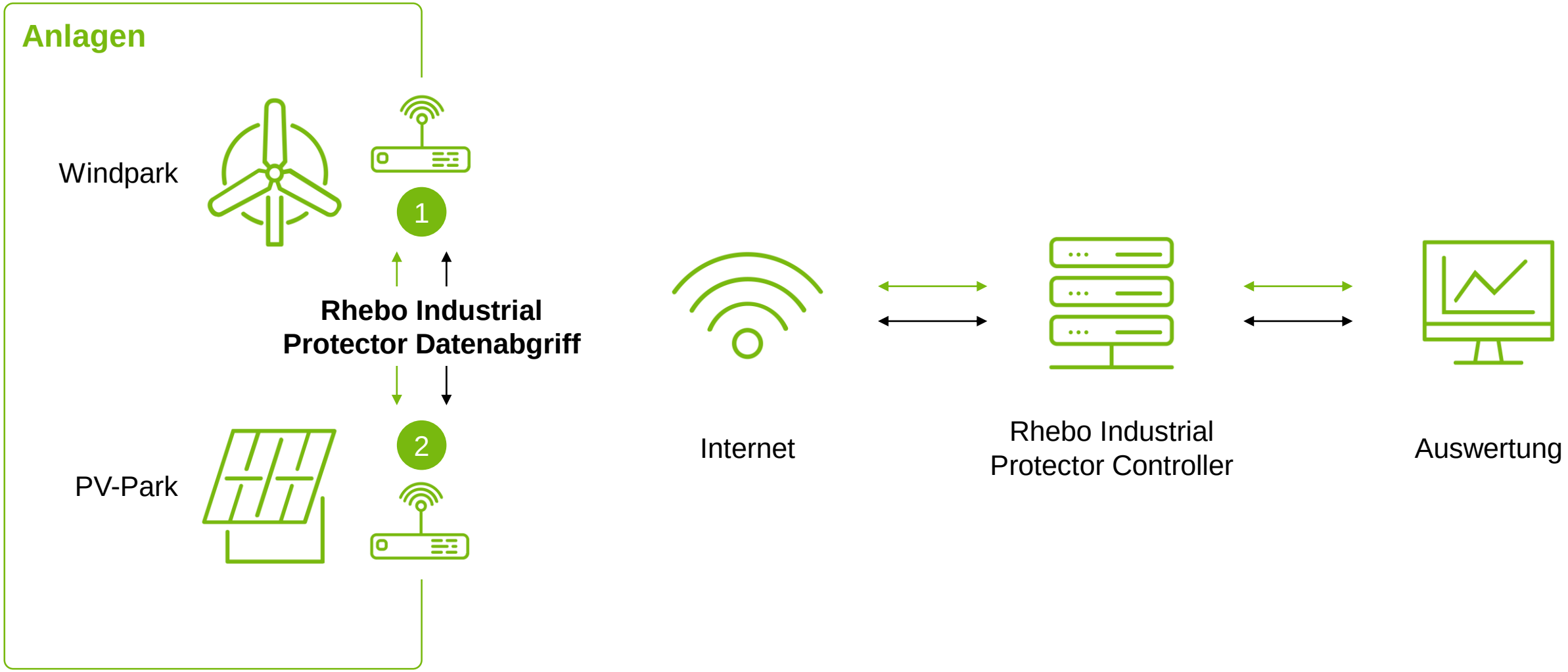
Spezielle Monitoringlösung für Steuerungsnetze (entsprechende Protokolle, Geräte, Anwendungen)

Rhebo ist der führende europäische Anbieter von Lösungen für Industrial Security und Continuity



Aufbau und Besonderheiten

Aufbau und Besonderheiten



Erkenntnisse

Anmeldung an ungeschützten FTP-Servern

Ungeeignete Software Version

- Serverversion ist veraltet (Stand 2006)
- Software enthält bekannte Sicherheitslücken
- Es wird eine Beta Version eingesetzt

Unverschlüsselte Verbindung

- Server ist aus dem öffentlichen Internet erreichbar
- Benutzer und Passwort werden im Klartext übertragen

Verwundbare Kommunikation mit externen SSH-Servern

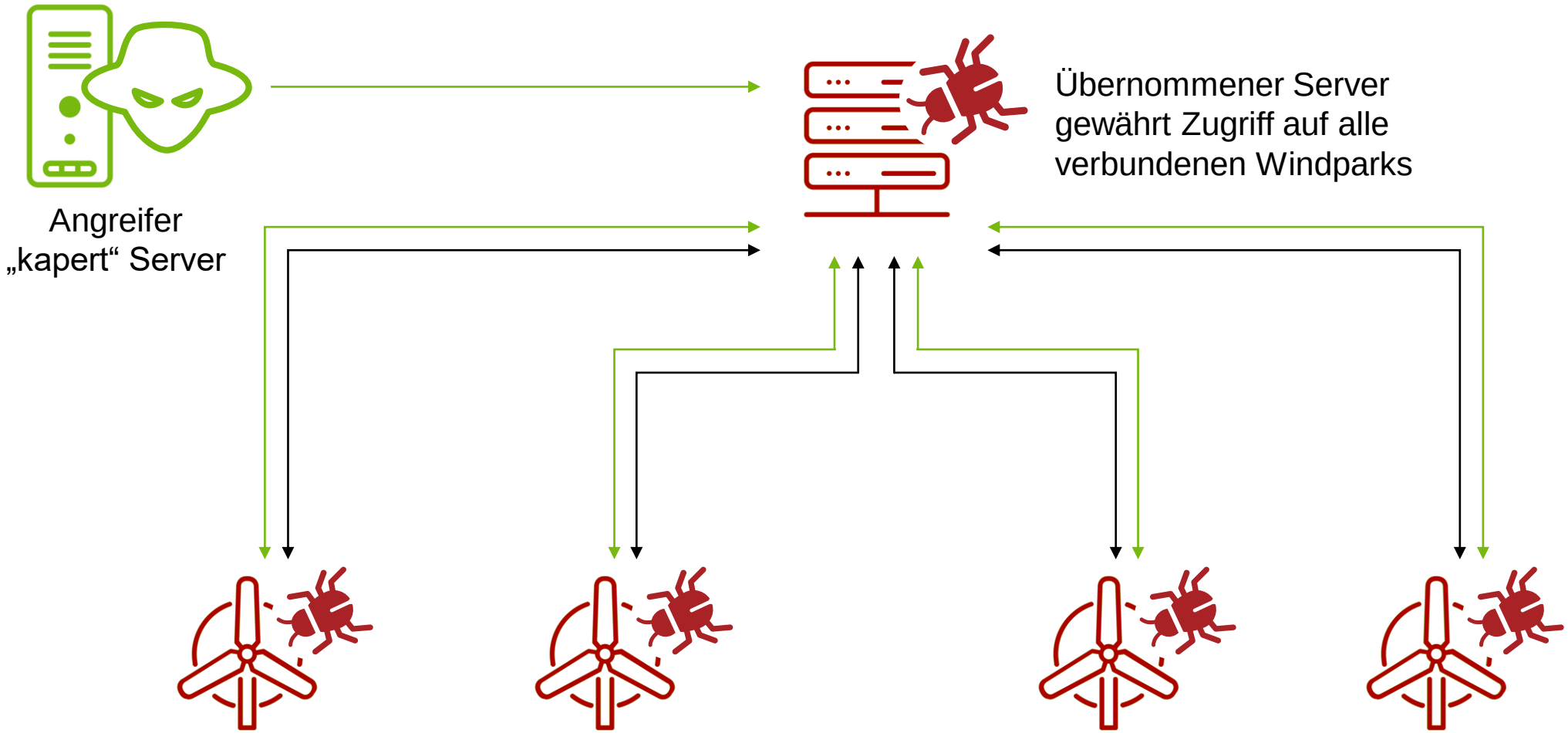
Veraltete Server-Software

- Serverversion ist veraltet (Stand 07/2016 und 10/2009)
- Software enthält bekannte Sicherheitslücken die aktiv ausgenutzt werden
- Server ist aus dem öffentlichen Internet erreichbar
- Ein „Hack“ des Servers hätte weitreichende Folgen

Veraltete Client-Software

- Die Software auf den Geräten im Park war ebenfalls veraltet (Oktober 2014)
- Damit ist ein Angriff auf die Infrastruktur des Parks möglich

Möglicher Angriff über verwundbare SSH-Server



Private Kommunikation

Private Kommunikation über das Parknetzwerk

WhatsApp

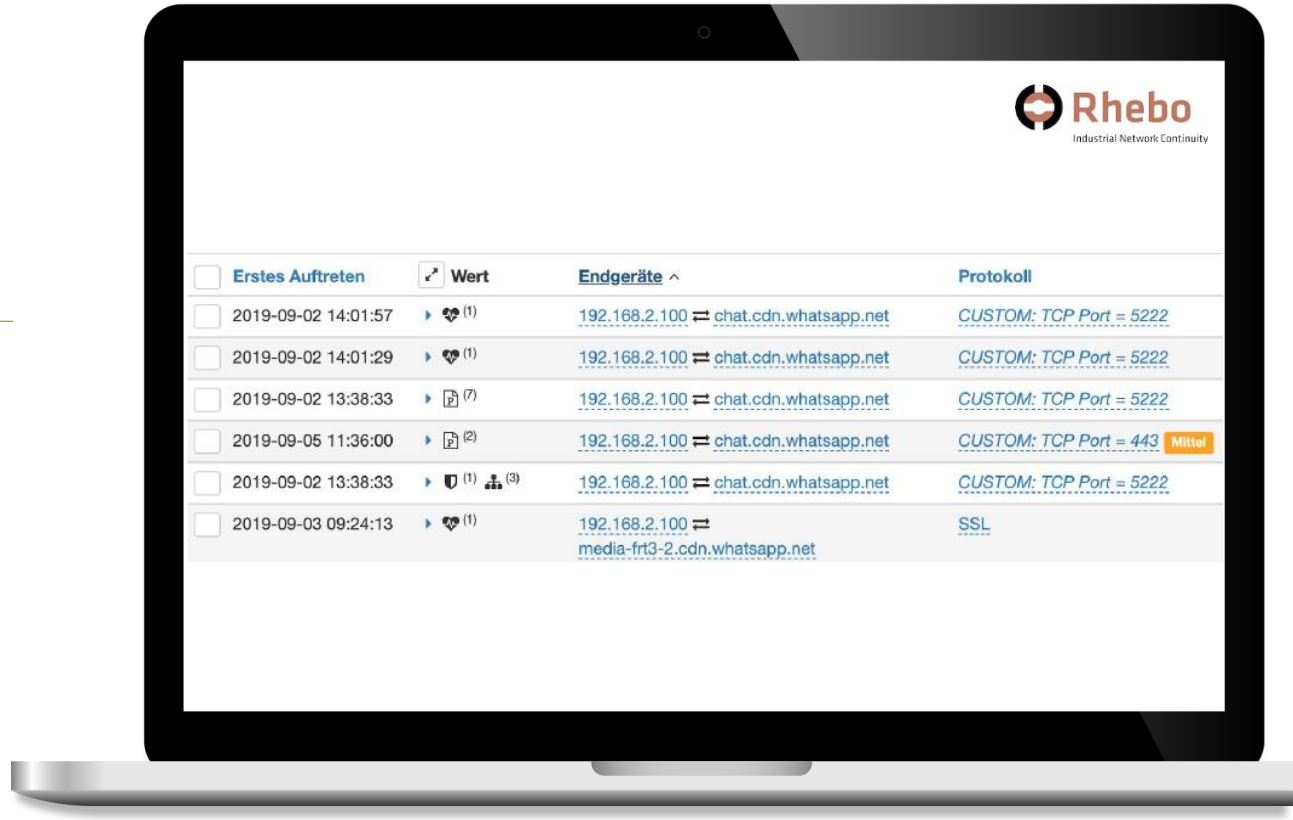
Skype

Google Talk

Diverse Internetseiten

Mögliche Folgen

- Private Nutzung birgt immer Risiken
- Viren und andere Malware können so unbeabsichtigt auf das Anlagennetzwerk übergreifen
- Angreifer können über kompromittierte Hardware (Notebook, Smartphone) Zugriff auf das Parknetzwerk erlangen
- Erhöhung des Datenverbrauchs des Parks



Nicht benötigte Protokolle

3

Der Fund hilft das Netzwerk besser abzusichern

2

Das gefundene Protokoll ist immer wieder von Sicherheitslücken betroffen

1

Software hat z.B. ein Protokoll entdeckt das nicht benötigt wird aber ein potenzielles Sicherheitsrisiko darstellt

Kein direktes Sicherheitsrisiko,
aber kann direkt ausgenutzt werden

!

PC vor Ort nutzt
unnötiges Protokoll

Netzwerkqualität

01

Datenverkehr trotz Reset

- Einige Geräte sendeten Daten obwohl es einen Reset-Befehl gab
- Scheinbar wurde der Befehl nicht empfangen
- Hinweis auf Fehler bzw. fehlerhafte Geräte im Netzwerk

02

Fehlerhafter Verbindungsaufbau

- Bei einigen Übertragungen kam es vor, dass die Daten für den Verbindungsaufbau nicht korrekt übermittelt wurden
- Scheinbar gibt es Probleme mit der Internetverbindung oder einem Netzwerkgerät
- Hinweis den man verfolgen muss, um die Qualität des Netzwerks zu verbessern

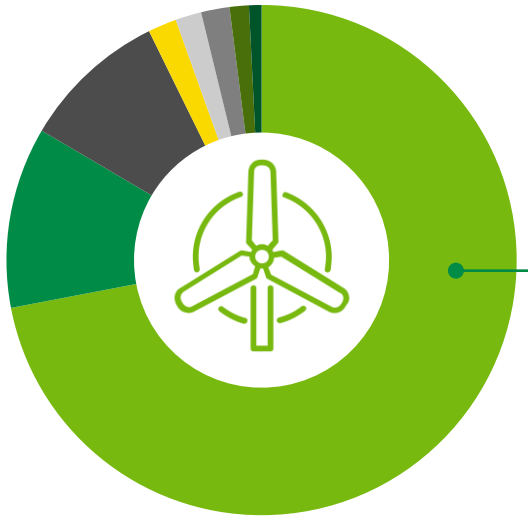
03

Ungewöhnliches Verhalten von Datenloggern

- Einige Datenlogger fragten die Zeit bei ca. 100 verschiedenen Servern ab und zeigten auch an anderen Stellen ungewöhnliches Verhalten
- Kein akutes Sicherheitsproblem, der Hersteller wurde auf das Verhalten aufmerksam gemacht

Auswertung Datenverbrauch, September 2019

Windpark

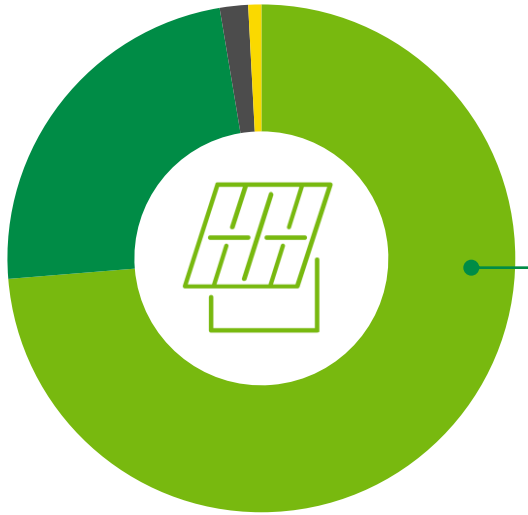


72%

Hersteller

- Hersteller 72,00%
- Eisansatzerknnung 11,47%
- Monitoring 9,26%
- Unbekannt A 1,81%
- Unbekannt B 1,65%
- Google DNS 1,80%
- Private Nutzung 1,22%
- Sonstige 0,79%
- Gesamt 13GB

PV-Park

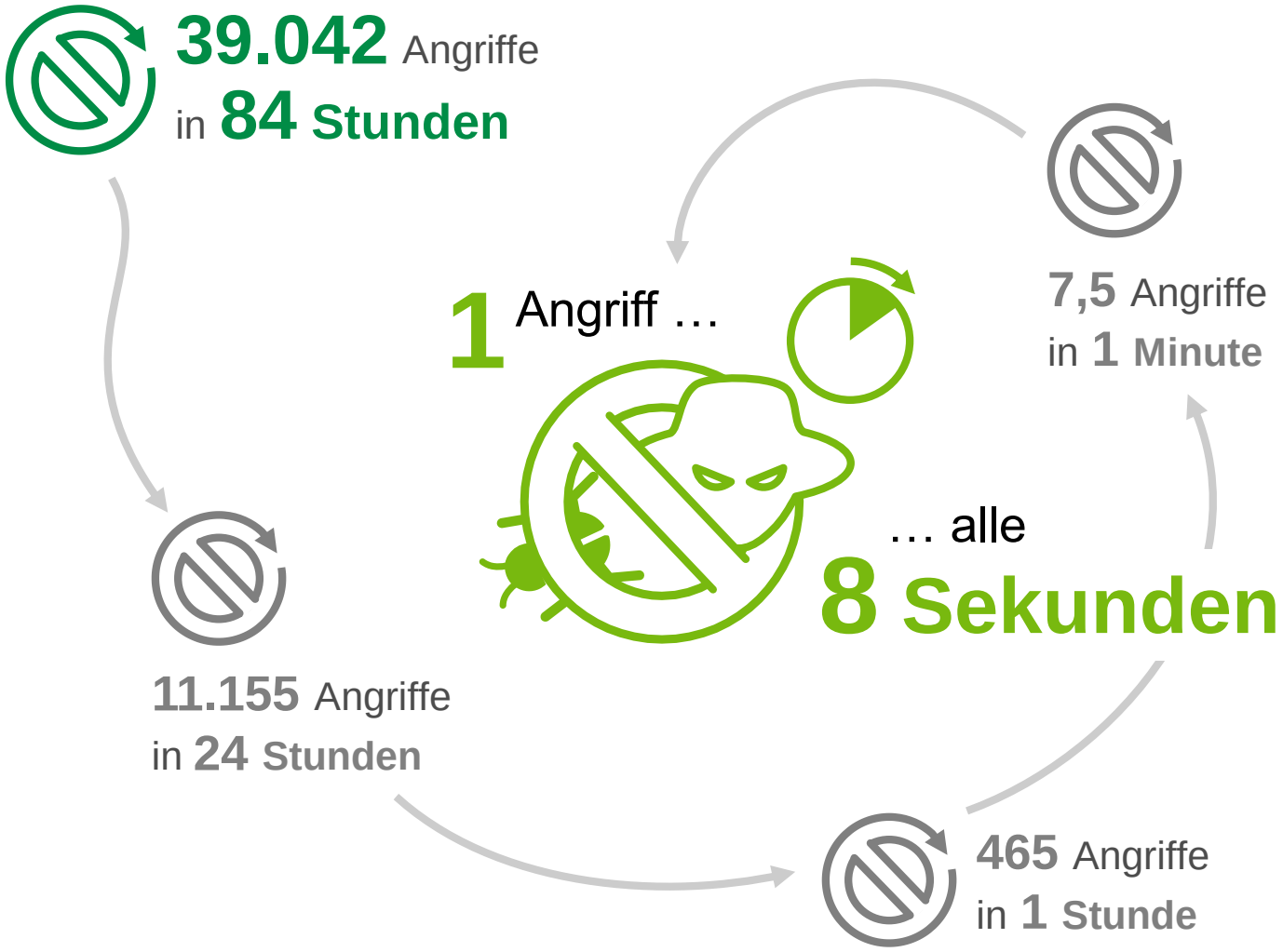


73%

Portal A

- Portal A 73,71%
- Portal B 23,66%
- Direktvermarkter 1,80%
- Sonstige 0,83%
- Gesamt 3,5GB

Auswertung Angriffe



Herkunft

- Angreifer stammten aus unterschiedlichsten Ländern (Russland, China, Moldawien, Spanien, Indien etc.)
- Hohe Anzahl russischer Server

Motivation

- Die meisten IP-Adressen waren als „Internet Scanner“ bekannt
- Einige waren scheinbar „private“ IP-Adressen
- Auch Server mit Sicherheits-lücken (teilweise 20 Stück!), die wahrscheinlich von einem Hacker übernommen wurden

Fazit

Fazit der Untersuchung

IT Sicherheit ist verbesserungswürdig

- Hersteller müssen ihre Server besser absichern und auf dem aktuellen Stand halten!
- Private Internetnutzung muss untersagt sein
- Man sollte immer ein „offenes Auge“ haben auf sein eigenes Netzwerk

Netzwerke sind gut aber ausbaufähig

- Aufbau und Struktur der Netzwerke ist OK, aber es gibt noch Verbesserungspotenzial
- Datenmenge könnte von den Herstellern sicherlich reduziert werden
- Nicht alle Geräte arbeiten so wie erwartet

Vielen Dank

Andreas Schmid, Rhebo GmbH

Head of Service & Support
Andreas.Schmid@rhebo.com

Mohamed Harrou, BayWa r.e.

Head of SCADA
Mohamed.Harrou@baywa-re.com

Copyright