Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

06.05. 2019

Leitfaden für Umsetzung des VSE-Handbuches für OT-Sicherheit in Kritischen Infrastrukturen der Schweiz

Von Rhebo GmbH

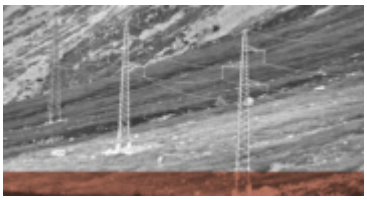


Bild Rechte
Rhebo GmbH

- **Rhebo veröffentlicht Leitfaden zum VSE »Handbuch Grundschutz für «Operational Technology» in der Stromversorgung«**
- **Leitfaden erörtert Umsetzung der 21 Schritte zum sicheren OT-Netz mittels Netzwerkmonitoring und Anomalieerkennung**
- **Empfehlungen orientieren sich an den konkreten Aufgaben der IT/OT-Sicherheit**

(Leipzig / Zürich)(PPS) Das *»Handbuch Grundschutz für «Operational Technology» in der Stromversorgung«* des VSE adressiert die Verantwortlichen der Sicherheit von Prozess- und Netzleitsystemen in Energieversorgungsunternehmen. Das Handbuch beschreibt und empfiehlt Maßnahmen, wie Energieversorgungsunternehmen die Sicherheit und Stabilität ihrer Prozess- und Netzleittechnik nachhaltig gewährleisten können.

Im Kern empfiehlt das Handbuch die Umsetzung des Defense-in-Depth-Konzepts. Zum einen liefert dieses Konzept den Verantwortlichen die Rahmenbedingungen, um die Informationssicherheit ihres Unternehmens kontinuierlich zu evaluieren, zu

beurteilen und zu verbessern. Zum anderen bietet das Konzept einen Lösungsansatz auf die Frage, wie in einer Welt, in der keine 100-prozentige Sicherheit möglich ist, Kritische Infrastrukturen bestmöglich gesichert werden können. In dem Handbuch heißt es dazu *»Ein Cyber-Angriff kann nicht verhindert werden – deshalb ist das Ziel die rasche Erkennung, Isolierung, Abwehr und Verringerung von Folgen einer Verletzung (Resilienz)«*

In 21 Schritten zur Defense in Depth

Der Leitfaden *»VSE-Handbuch in der Praxis«* von Rhebo unterstützt die Verantwortlichen in Kritischen Infrastrukturen insbesondere bei der Umsetzung der *»21 Schritte zum sicheren OT-Netz«*. Um die Alltagspraxis der IT/OT-Sicherheit in Kritischen Infrastrukturen zu berücksichtigen, werden die 21 Schritte im Kontext des kontinuierlichen Verbesserungsprozesses (Plan, Do, Check, Act) betrachtet, wie er für die Organisation eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27000 empfohlen wird. Im Fokus des Leitfadens steht dabei die Etablierung eines durchgängigen Netzwerkmonitorings mit industrieller Anomalieerkennung. Diese fungiert als Basis für die Risikoanalyse sowie die Identifikation, Meldung, Dokumentation und Analyse von Fehlerzuständen, Manipulationen, Schadsoftware und Sicherheitslücken.

Christian Schöpf, Sales Director Rhebo für die Schweiz und Österreich, erklärt dazu:

> »Betreiber Kritischer Infrastrukturen stehen vor der Herausforderung, die Vielzahl an Empfehlungen aus dem VSE-Handbuch und dem IKT-Minimalstandard in ein schlüssiges Konzept für ihre eigenen Anlagen zu überführen. Mit dem Leitfaden möchten wir die Verantwortlichen dabei unterstützen, die Empfehlungen im Kontext des Defense-in-Depth-Ansatzes zu verorten. Wir bei Rhebo sind überzeugt, dass Betreiber im Hinblick auf die vielschichtigen Gefährdungsvektoren und Verfügbarkeitsaspekte der komplexer werdenden Netzwerke den Blick auf das innere Wirken der Prozess- und Netzleittechnik richten müssen. Und das heißt nicht weniger, als ein System zu etablieren, dass alle Kommunikationsvorgänge innerhalb des Netzwerkes analysiert, Hinweise auf versteckte Sicherheitslücken gibt

> und Auffälligkeiten in Echtzeit meldet. Denn sowohl Advanced Persistent Threats als auch technische Fehlerzustände werden in der Regel nicht an den Netzwerkgrenzen erkannt, wo die Firewalls sitzen«.

Der Leitfaden *»VSE-Handbuch in der Praxis – Die Rolle von Netzwerkmonitoring und Anomalieerkennung beim stabilen Betrieb Ihrer Prozess- und Netzleittechnik«* ist kostenfrei erhältlich unter: https://rhebo.com/de/download/file/leitfaden-vse-handbuch-in-der-praxis/.

Über die Organisation:

Rhebo ist ein deutsches Unternehmen und hat sich auf die Ausfall- und Störungssicherheit von Industrieunternehmen und Kritischen Infrastrukturen spezialisiert. Mit seinen Lösungen und Services überwacht Rhebo die Datenkommunikation innerhalb der Steuerungstechnik und meldet zuverlässig Angriffe, Schwachstellen sowie technische Fehlerzustände.

Rhebo unterstützt konkret Betreiber von Industrial Control Systems, Netzleittechnik und Leitsystemen, die Cybersicherheit, Produktivität und Verfügbarkeit ihrer Anlagen zu steigern und die digitale Transformation der Prozesse zu sichern.

Das Unternehmen engagiert sich in dieser Rolle aktiv bei der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem Teletrust – Bundesverband IT-Sicherheit e.V. und dem Bitkom Arbeitskreis Sicherheitsmanagement bei der Erarbeitung von Standards und Handlungsempfehlungen.

Pressekontakt:

Public Relations
Jens Pacholsky
Tel. +49-341-393-790-180
press @ rhebo.com

Spinnereistraße 7
04179 Leipzig
Deutschland

Rhebo Suisse
Christian Schöpf
Tel. +41 76 341 78 79
christian.schoepf @ rhebo.com

Jupiterstr. 49
CH 8032 Zürich
Schweiz

Kategorie
Umwelt & Energie

Source URL: *https://www.presseportal-schweiz.ch/pressemeldungen/leitfaden-fuer-umsetzung-des-vse-handbuches-fuer-ot-sicherheit-kritischen*