Pressemitteilung

IT-Sicherheitsgesetz einhalten

Bahnanwendungen mit IT-Sicherheitsanalyse vor Angriffen schützen

Stuttgart, 14. Mai 2017 - **Das diesjährige Muttertagswochenende war geprägt von Nachrichten über den WannaCry Malware-Angriff, der sich in fast 100 Länder ausbreitete. Auch deutsche Unternehmen waren betroffen. Sicherheitsexperten sehen hierin eine Eskalation der weltweit wachsenden Bedrohung für unsere zunehmend digitalisierte Infrastruktur. Dies macht erneut deutlich, dass die Bundesregierung mit dem IT-Sicherheitsgesetz zu Recht Betreiber kritischer Infrastrukturen (KRITIS) dazu verpflichtet, ihre Systeme nach dem Stand der Technik zu schützen. Wie dies auf Grundlage vertrauter Normen und Vorgaben im Transportwesen möglich ist, erklärt ein Artikel am Beispiel einer Leit- und Sicherungstechnik (LST) für Bahnanwendungen.**

Der Autor Patric Birr, RAMS Engineer bei der ICS AG, beschreibt in seinem Artikel das Vorgehen zur Ableitung von IT-Sicherheitsanforderungen. Dabei werden sowohl an die Organisation und Prozesse von Bahnbetreibern als auch an die Technik der dazugehörigen LST- Systeme Anforderungen gestellt. In Bahnanwendungen müssen dem Stand der Technik entsprechende IT-Sicherheitsanforderungen umgesetzt und kontinuierlich überprüft werden. Um dies zu gewährleisten, muss zuerst auf Basis der gängigen Sicherheitsnormen ein System zur Risikobewertung errichtet und zertifiziert werden. Darauf aufbauend folgt die Einführung und ebenfalls Zertifizierung entsprechender Schutzmechanismen.

Vom bahnspezifischen Leitfaden zur Zertifizierung

Birr erklärt, wie eine IT-Sicherheitsanalyse auf Basis der bekannten Normenreihe IEC 62443 zum Schutz von industriellen Kommunikationsnetzen durchgeführt werden kann. Das im bahnspezifischen Leitfaden DIN VDE V 0831-104 beschriebene Vorgehen zur Anwendung der Normenreihe wird dabei um eine mehrstufige qualitative Risikobetrachtung erweitert. Dies geschieht durch die Anwendung bewährter „Bottom-Up“- und „Top-Down“-Analysetechniken, die schrittweise die vorhandenen Schutzmechanismen bewerten und gegebenenfalls ergänzen.

Um, wie von dem IT-Sicherheitsgesetz gefordert, dem Stand der Technik zu entsprechen, empfiehlt der Autor, Datenbanken wie die vom BSI erstellten IT-Grundschutzkataloge zu Rate zu ziehen und mit IT-Experten zusammenzuarbeiten. Wenn im System die geforderten IT-Sicherheitsanforderungen implementiert und die entsprechenden Nachweise erbracht sind, steht einer Systemzertifizierung nichts mehr im Wege. Dadurch kann eine Schädigung der Systeme durch Malware wie WannaCry, abgewendet werden.

Der Artikel ist in Signal+Draht, Ausgabe 4/2017 erschienen.

(Autor: Julia Grewe)

Pressemitteilung

Über die ICS AG:
Die ICS AG ist seit mehr als 50 Jahren ein erfolgreiches, familiengeführtes IT-Beratungs- und Engineeringunternehmen. Die Spezialisierung liegt in den Geschäftsfeldern Industrial Engineering (Automation, Supply Chain, Logistic, Automotive), Transportation und Research und Development. In den Bereichen Funktionale Sicherheit, Security & Safety sowie KRITIS sorgt die ICS AG für intelligente und sichere Prozesse in komplexen Umgebungen.

Pressekontakt:	**Fachlicher Kontakt**
ICS AG Marketing & PR **Frau Stefanie Henzler** Sonnenbergstraße 13 70184 Stuttgart Tel.: +49 711 21037 – 40 Fax:+49 711 21037 – 53 Web: www.ics-ag.de E-Mail: press@ics-ag.de	ICS AG Leiter Geschäftsfeldentwicklung **Herr Michael Kirsch** Sonnenbergstraße 13 70184 Stuttgart Tel.: +49 711 21037 – 00 Fax: +49 711 21037 – 53 Web: www.ics-ag.de E-Mail: kritis@ics-ag.de

Weitere Informationen und hochauflösende Bilder für die Presse schicken wir Ihnen gerne auch auf Wunsch zu. Zur Veröffentlichung, honorarfrei. Belegexemplar oder Veröffentlichungshinweis wäre sehr freundlich.