Pressemitteilung

CYSIS:
Bahnindustrie und Wissenschaft erarbeiten IT-Sicherheitskonzepte

Die Signale stehen auf Sicherheit:
Das IT-Sicherheitsgesetz und die Bahnindustrie

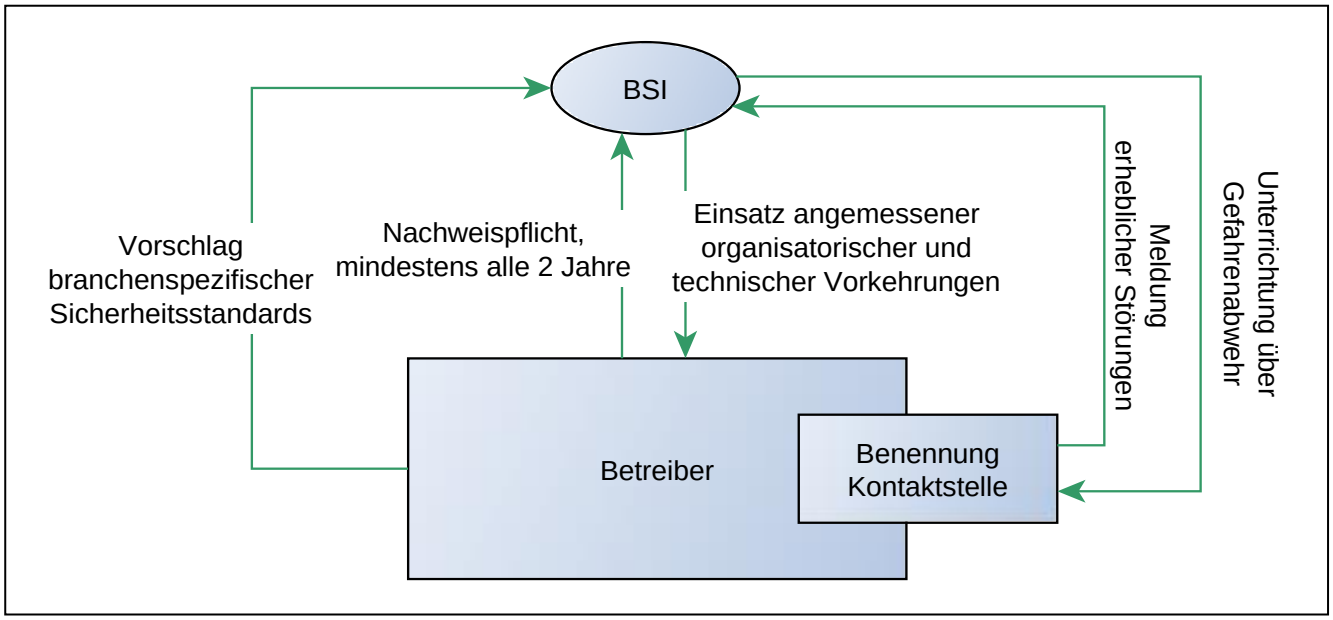
Stuttgart, 4. Juli 2017 - **Kostenfreies WLAN in ICE-Zügen, vollautomatische Schienenfahrzeuge - die Bahnbranche treibt mit großen Schritten die Digitalisierung voran. Doch wie können Bahnbetreiber und Zulieferer in Zeiten von WannaCry & Co. sicherstellen, dass Hacker bei ihnen keine Chance haben? Wie passen Safety und Security zusammen und gewährleisten auch bei IT-Sicherheitsvorfällen ein reibungsloses Fortführen des Betriebs? Und welche Vorgaben macht das IT-Sicherheitsgesetz? Mit diesen Themen beschäftigt sich seit Anfang 2016 die Forschungskooperation Cyber-Security für sicherheitskritische Infrastrukturen (CYSIS). Die ICS AG aus Stuttgart ist aktiv dabei.**

Mit der fortschreitenden Digitalisierung werden Anlagen und Fahrzeuge mit komplexen Softwaresystemen kombiniert und an öffentliche Netze angebunden. *„Früher hatte man eigene Server-Systeme und Netze. Heute muss man sich mit Cyberkriminalität auseinandersetzen“*, warnt Andreas Langer, Key Account Manager Transportation bei der ICS AG. Obwohl sich dieses Bewusstsein in der Bahnbranche in den letzten zwei bis drei Jahren geschärft hat, ist es immer noch ein weiter Weg zur Umsetzung von Sicherheitsmaßnahmen.

Die Zeit drängt: IT-Sicherheit ist ein komplexes Thema

Ziel von CYSIS ist der Informationsaustausch zwischen Industrie und Wissenschaft, um die Security in den sicherheitskritischen Strukturen der Bahnbetreiber zu verbessern. Dazu gehört auch die Umsetzung der Vorgaben aus dem IT-Sicherheitsgesetz, das Betreiber kritischer Infrastrukturen (KRITIS) in die Pflicht nimmt. Nach der Verabschiedung der für die Bahnindustrie geltenden BSI-Verordnung haben Betreiber zwei Jahre Zeit, konkrete Sicherheitsmaßnahmen zu implementieren. *„Die Betroffenen denken, dass sie sich Zeit lassen können“,* weiß Andreas Langer aus Erfahrung. *„Dabei wird die Komplexität des Themas unterschätzt.“*

Das IT-Sicherheitsgesetz schreibt nicht vor, welche Normen und Vorschriften angewendet werden sollen. Es verweist lediglich auf den „neuesten Stand der Technik“.



Patric Birr, RAMS Engineer bei der ICS AG meint: *„Bei CYSIS sitzen alle Beteiligten am selben Tisch um Lösungsansätze zu diskutieren und dabei geeignete Standards für die Branche zu identifizieren.“* Bislang wird die bahnspezifische Vornorm DIN VDE V 0831-104 angewendet. *„Die international anerkannte Normenreihe für industrielle Kommunikationsnetze ISO/IEC 62443 wird aber immer konkreter und vollständiger“*, so Birr. Ein IT-Sicherheitsnachweis in Anlehnung an den neu entstehenden Teil ISO/IEC 62443-3-2 (IT-Sicherheits- Risikobewertung für Systementwicklung) funktioniert sehr gut. Birr: *„Bei der ICS AG haben wir ein entsprechendes Vorgehensmodell bereits erfolgreich angewendet.“*

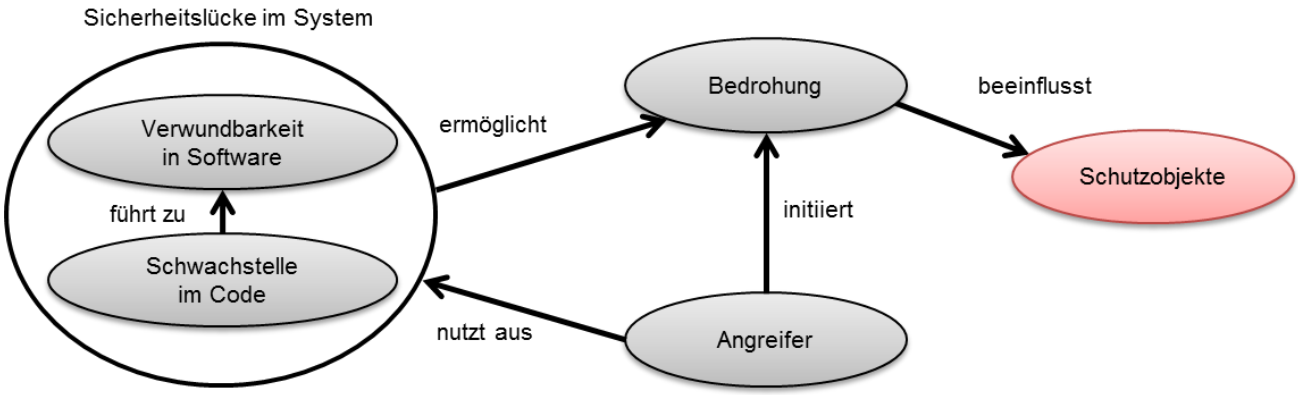
Alles sicher? Security für Safety

Wie Patric Birr erklärt, stand im Bahnsektor bislang die funktionale Sicherheit (Safety) an erster Stelle. Safety stellt sicher, dass Anlagen und Fahrzeuge jederzeit einen definierten Zustand haben und somit ein ungestörter Betrieb gewährleistet ist. Bei der Komplexität und Dynamik heutiger Softwaresysteme reicht dieser Ansatz zumeist nicht mehr aus. Safety muss mit etablierten Verfahren der Security ergänzt werden.

Der Cyber-Angriff mit der Malware WannaCry auf die Anzeigen der Bahn hat gezeigt, dass viele Systeme inzwischen von außen manipulierbar sind. „Das Ausfallen der Anzeigen war zwar ärgerlich aber nicht kritisch“, bemerkt Andreas Langer. Kritisch wird es allerdings, wenn Cyber-Kriminelle über eine unzureichende Trennung von Anzeigensystem und Signalsteuerung die Kontrolle über den Fahrweg übernehmen können.

Der Betrieb und die Zulassung der Systeme ist auf eine Nutzung von mitunter 20-30 Jahre ausgelegt. Die Zulassung der Systeme durch das Eisenbahn-Bundesamt (EBA) bleibt aber aktuell nur bestehen, wenn keinerlei Anpassungen an den Systemen vorgenommen werden. Um mit den aus Security-Gründen u.U. regelmäßig erforderlichen Änderungen an Softwaresystemen handlungsfähig zu

bleiben, ist es notwendig, die Security technisch klar von der Safety zu trennen und auch den Zulassungsprozess entsprechend zu adaptieren. Die Safety-Funktionen der Systeme werden dafür in eine Security-Schale eingebettet, die dynamischer an die aktuelle Bedrohungslage angepasst werden kann. In einem umfassenden IT-Sicherheitsnachweis ist die Rückwirkungsfreiheit der Security gegenüber dem sicherheitsrelevanten System nachzuweisen.



Patric Birr hat ein Vorgehensmodell erarbeitet, das sowohl in der Entwicklung als auch später im Betrieb dynamisch die Gegenüberstellung neuer Angriffsmuster mit geeigneten Schutzmaßnahmen ermöglicht. Damit wird sichergestellt, dass nach jedem Software-Update oder Patch die Voraussetzungen für die EBA-Zulassung immer noch gegeben sind. Der zeit- und kostenaufwendige Prozess einer Neuzulassung ist nicht erforderlich.

Der Letzte macht die Türe zu: ganzheitliche IT-Sicherheit

„Die beste Technik nutzt nichts, wenn organisatorisch und infrastrukturell die IT-Sicherheit nicht hergestellt ist“, warnt Patric Birr. Bei CYSIS konnte er vermitteln, dass IT-Sicherheit nur in einem ganzheitlichen Ansatz funktioniert. Dazu müssen neben der Technik auch der Betrieb, die Infrastruktur und das Personal in die Betrachtung mit einbezogen werden. Als Standard hat sich hierzu die Reihe ISO/IEC 2700x bewährt. Sie bezieht sich auf Managementaspekte und legt Richtlinien und allgemeine Grundsätze für die Einführung, Umsetzung, Aufrechterhaltung und Verbesserung des Informationsmanagements innerhalb einer Organisation fest.

Andreas Langer verspricht sich von der Mitarbeit bei CYSIS, dass Unternehmen für das Thema IT-Security weiter sensibilisiert werden und zeitnah die geforderten Maßnahmen angehen. *„Allen ist klar, dass sich Cyber-Attacken nicht verhindern lassen“*, sagt Langer. Aber es ist wichtig, die gesetzlichen Vorgaben umzusetzen. Und das ist ein langer Prozess. Dass hiervon nicht nur die großen Bahnbetreiber und Produzenten betroffen sind, ist den wenigsten bewusst. *„Zwar ist der Betreiber für die Sicherheit seiner Anlagen verantwortlich“*, sagt Langer, doch beim Zukauf von Komponenten geben die Bahnbetreiber ihre Sicherheitskriterien an Lieferanten und Sublieferanten weiter. *„Da wir uns bei der ICS AG schon sehr lange mit dem Thema beschäftigen, können wir für CYSIS einen wertvollen Beitrag leisten“*, ist Langers Einschätzung.

Infokasten:

Das IT-Sicherheitsgesetz

Am 31. Mai hat die Bundesregierung der Änderung der BSI-KRITIS-Verordnung zugestimmt. Sie legt die Kriterien fest anhand derer Betreiber Kritischer Infrastrukturen aus den Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr überprüfen können, ob sie unter das IT-Sicherheitsgesetz fallen.

Damit kann die Verordnung im Juni 2017 in Kraft treten.

Ab jetzt haben die betroffenen Unternehmen für die Umsetzung zwei Jahre Zeit.

Die Regelungen für die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser und Ernährung sind bereits seit Mai 2016 in Kraft.

Für Betreiber Kritischer Infrastrukturen in der Transportbranche gelten folgende Schwellwerte:

- Schienennetze, Stellwerke und Leitzentralen im ÖSPNV: ab 125 Mio. beförderten Personen im Jahr oder 500.000 Einwohner in der überwachten Region
- Personenbahnhöfe der jeweils höchsten Kategorie
- Güterbahnhöfe und Zugbildungsbahnhöfe: ab 23.000 Züge im Jahr
- Logistikzentren und Umschlaganlagen: ab 17 Mio. Tonnen Güter im Jahr
- Abfertigungsanlagen und Flughäfen: ab 20 Mio. Passagiere im Jahr bzw. 750.000 Tonnen Fracht im Jahr
- Flugsicherung und Luftverkehrskontrolle: ab 17.5000 Flugbewegungen im Jahr

Es wird allerdings erwartet, dass die betroffenen Unternehmen von ihren Zulieferern entsprechende Garantien oder Zertifizierungen verlangen.

Die vom BSI vorgegebenen Richtlinien beinhalten folgende Maßnahmen:

- Einhaltung eines Mindestniveaus an IT-Sicherheit
- Nachweis der Erfüllung durch Sicherheitsaudits
- Meldepflicht für erhebliche IT-Störungen
- Betreiben einer Kontaktstelle innerhalb des Unternehmens zum BSI

Patric Birr ist aktiv in den CYSIS Arbeitsgemeinschaften *Security for Safety* und *ETCS mit Security* vertreten.

Pressemitteilung

Von Patric Birr ist erschienen: „Vorgehensmodell zur IT-Sicherheitsanalyse für Bahnanwendungen“ in Signal+Draht, Ausgabe 4/2017.

Andreas Langer und Patric Birr nehmen am CYSIS Cyber Congress am 4. Juli 2017 in Frankfurt teil.

(Autor: Julia Grewe)

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.