Cybersicherheit einfach gemacht

Wie Prozessleitsysteme noch sicherer, konformer und zuverlässiger werden.

Cyberangriffe auf industrielle Infrastruktur sind eine Tatsache, der man sich stellen muss. Sie kommen mit zunehmender Häufigkeit vor und sind ein globales Phänomen. In der Europäischen Union zum Beispiel summieren sich die Verluste, die durch diese Angriffe verursacht werden, auf bis zu 1,6 % des Bruttoinlandsprodukts – was Dutzenden von Milliarden Euro jährlich entspricht. Nebst dem Finanzsektor sind vor allem Informations- und Kommunikationstechnik (IKT) sowie der Energiesektor betroffen, einschliesslich der Stromerzeugung. Etwa die Hälfte aller Attacken in der EU haben zum Ziel, den Betrieb durch Denial of Service (DoS) durch eine Überlastung des Netzes zu stören, etwa durch Vielanfragen aus mehreren Quellen (Distributed Denial of Service – DDoS).

Einen Überblick über die täglich registrierten Cyberattacken ist auf www.digitalattackmap.com zu sehen. Diese Website zeigt Livedaten von DDoS-Vorfällen auf der ganzen Welt. So wurden zum Beispiel allein am 25. August 2016 grossangelegte DDoS-Attacken in den USA, in Chile, Irland, Grossbritannien, Dänemark, Rumänien, Saudi-Arabien und Hongkong registriert, ebenso eine ungewöhnlich hohe Anzahl versuchter Störungen auf der Kanalinsel Jersey, den Philippinen, in Marokko und Mosambik.

Cyberangriffe sind nun so verbreitet, dass das US-amerikanische «National Cybersecurity and Communications Integration Center» in einem Bericht schreibt: «Bei vielen industriellen Steuerungssystemen stellt sich nicht die Frage, ob ein Eindringen stattfinden wird, sondern, wann das passiert.» Der gleiche Bericht listet sieben Strategien auf, durch die Unternehmen ihre Steuerungssysteme vor 98 % aller Vorfälle schützen können. Allein drei dieser Strategien würden 84 % der Cyberattacken verhindern. Diese drei Strategien sind:

- Implementierung einer Anwendungsweissliste, um die Ausführung unbefugter Programme zu verhindern;
- sicherstellen, dass ein ordnungsgemässes Patch-Management-Programm installiert ist;
- Verringerung der Angriffsempfindlichkeit des Kontrollsystems, indem es von nicht vertrauenswürdigen Netzwerken wie dem Internet isoliert wird.

Cybersicherheits-Compliance

In vielen Ländern ist das Einhalten der Richtlinien der nationalen Regulierungsbehörden der Hauptgrund, weshalb Kraftwerksbetreiber ihre Cybersicherheit stärken, manchmal auch das Einhalten der Mindestanforderungen von IT-Unternehmen oder der IT-Abteilung des Kraftwerkunternehmens.

Während viele Unternehmen und Anlagen bereits ein hohes Mass an Sicherheit erreicht haben und über die Fähigkeiten wie auch Verfahren verfügen, um es zu pflegen, gibt es so manche andere, die nicht über die Expertise und Werkzeuge verfügen, um diese Richtlinien oder Anforderungen zu erfüllen. Hier kann ABB einen erheblichen Mehrwert beisteuern und den Kunden helfen, ihr Compliance-Programm umzusetzen und die erforderlichen Regulierungsrichtlinien oder IT-Anforderungen zu erfüllen – einschliesslich der sieben erwähnten Strategien des «US National Cybersecurity und Communications Integration Centers».

Einzigartiges Fachwissen

ABB hat eine einzigartige Position im Bereich der Leitsysteme, vor allem für kritische industrielle Infrastruktur. Das Unternehmen ist gemäss der ARC Advisory Group der weltweit führende Anbieter von Leitsystemen, insbesondere für die Grossindustrie wie Stromerzeugung, Öl und Gas, Zellstoff und Papier, Bergbau und Metalle. Diese Automatisierungs- und Prozesskompetenz in Kombination mit dem langjährigen Know-how in der Systemsicherheit ermöglicht es ABB, das Cyberrisiko für die Steuerungssysteme und Produktionsprozesse der Kunden zu minimieren.

Die Philosophie von ABB basiert im Wesentlichen auf zwei Strängen:

- Mit den Kunden zusammenzuarbeiten, um eine detaillierte Verteidigungsstrategie zu kreieren, in der mehrere Verteidigungsebenen Bedrohungen erkennen und abwenden;
- Cybersicherheit in jedes Stadium des Leitsystemproduktlebenszyklus einzubetten, von der Planung über die Entwicklung bis hin zu Betrieb und Wartung.

Security Workplace

Ein wichtiger Bestandteil des Cybersecurityangebots von ABB ist «Security Workplace», das speziell für die Stromerzeugungsindustrie entwickelt wurde. Es hilft Kunden mit Systemen von ABB oder von weiteren Anbietern, die Compliance der Cybersicherheit zu erreichen und zu erhalten, ohne die Systemzuverlässigkeit zu gefährden. Security Workplace umfasst eine integrierte Sammlung von Sicherheitsanwendungen und Tools zur Bewertung und Verstärkung des Leitsystemcyberschutzes. Dazu gehören:

Auf lokaler Ebene hat jeder der acht Stromerzeugungs-Service-Hubs von ABB Cybersecurity-Know-how, mit detaillierten Kenntnissen der lokalen Regulierungsbehörden und Stromerzeugungsmärkte – auch in der Schweiz.

- Automatisieren von wiederkehrenden händisch auszuführenden Aufgaben wie etwa grundlegende Cyber Security Wartung: Patch- und Virenscanner-Verwaltung und Verteilung/Systemhärtung (Hardening)/Datensicherung und Wiederherstellung (Backup – Restore)/ Erkennen von Unregelmässigkeiten im Netzwerk (Network Anomaly Detection)/Whitelisting /Auswertungen zur Konformität (Compliance Reporting);
- einfache Benutzerführung von zentraler Stelle mit vorkonfigurierte Funktionen;
- Unterstützung für die Sicherheits-Patch-Installation mit Datenträger (DVD);
- einheitliches Vorgehen auch bei unterschiedlichen Automatisierungssystemen möglich;
- erlaubt spezifische Lösungen zu implementieren, die sich aus Vorschriften oder anderen Bedürfnissen entwickeln.

Eine der Stärken der Cybersicherheitsressourcen von ABB besteht in deren globaler wie auch lokaler Verankerung. Auf globaler Ebene spielt ABB seit Langem eine aktive Rolle bei der Definition und Umsetzung von Cybersecuritystandards für Strom- und Industriesteuersysteme. Und die unabhängig betriebene «Device Security Assurance Center» prüft die Robustheit und Widerstandsfähigkeit der Geräte, die ABB in die Steuerungssysteme eingebettet hat.

Auf lokaler Ebene hat jeder der acht Stromerzeugungs-Service-Hubs von ABB Cybersecurity-Know-how mit detaillierten Kenntnissen der lokalen Regulierungsbehörden und Stromerzeugungsmärkte. ABB ist also bestens dafür gerüstet, Kunden bei ihren Cybersicherheitsproblemen zu helfen.

Ein sicheres System ist zuverlässiger

Wenn ABB die Kunden bittet, «Security Workplace» zu bewerten, fällt als häufigste Antwort, dass «damit unser Leitsystem besser läuft.» Das ist nicht so überraschend, wie es klingen mag, denn die Erhöhung der Cybersicherheit eines Leitsystems erfordert die Aktualisierung kritischer Teile sowie ein Finetuning der Systemleistung. Ein sicheres System ist definitionsgemäss effizienter und zuverlässiger als ein nicht sicheres.

Weitere Infos: plantcontrol.support@ch.abb.com

ABB Security Workplace

Für Sicherheit, Compliance und Zuverlässigkeit

- Ein einziges, umfassendes Tool für die Cybersicherheit von Leitsystemen
- Minimiert die Angreifbarkeit des Systems, erhöht dessen Zuverlässigkeit
- Vereinfacht die Erfüllung der regulatorischen Vorgaben
- Weltweit unterstützt durch Cybersecurityexperten von ABB in acht regionalen Hubs.