

Phoenix Contact erhält Zertifikat vom TÜV Süd

Categories : [Hannover Messe](#), [Messtechnik](#)

Date : 8. April 2019

Phoenix Contact wurde vom TÜV Süd als eines der ersten Unternehmen in Deutschland nach der Normreihe für IT-Sicherheit IEC 62443-4-1 und 2-4 zertifiziert. Dies bestätigt, dass das Unternehmen:

- die Entwicklung von Secure-by-Design-Produkten entsprechend dem Prozess IEC 62443-4-1, sowie
- das Design von sicheren Automatisierungslösungen entsprechend dem Prozess IEC 62443-2-4

durchführt.

Diese Zertifizierungen unterstreichen die Strategie von Phoenix Contact, standardisierte Security in Produkten, Industrielösungen und Beratungsdienstleistungen anzubieten, um einen zukunftssicheren Betrieb von Maschinen, Anlagen und Infrastrukturen zu ermöglichen.

Bei Secure-by-Design-Produkten werden Sicherheitsanforderungen an Soft- und Hardware schon während der Entwicklungsphase eines Produktes berücksichtigt. So werden spätere Sicherheitslücken verhindert. Diese Sicherheitsmechanismen werden immer wichtiger, da Geräte und Sensoren zunehmend über das Internet vernetzt sind. Da immer mehr Prozesse über Software laufen, öffnen sich neue Angriffsflächen.

Die zentralen Elemente in der Norm zur IT-Sicherheit Teil 4-1 und 2-4 sind zum einen eine Bedrohungs- und Risikoanalyse auf Basis des Anwendungsszenarios. D.h. es werden für Geräte und Systeme Anwendungsbeispiele und die erforderlichen Härtnungsmaßnahmen festgelegt. Für Automatisierungslösungen wird ein Sicherheitskonzept mit den erforderlichen Schutzmaßnahmen erarbeitet. Zum anderen wird ein Produkt- oder Lösungsentwicklungsprozess etabliert, mit dem sicher nachvollzogen werden kann, dass alle identifizierten Security-Anforderungen implementiert, verifiziert und dokumentiert werden.

Zusätzlich sind Gerätehersteller dazu aufgefordert, auf Security-Schwachstellen angemessen zu reagieren und verlässlich Security-Updates zu veröffentlichen. Diese Anforderung wird bei Phoenix Contact durch das neu etablierte Product Security Incident Response Team (PSIRT) übernommen. Dieses Team informiert Anwender von Phoenix Contact-Produkten über bekannte Sicherheitslücken und ist zur gleichen Zeit die Stelle, bei der Anwender gefundene Sicherheitslücken vertraulich melden können. PSIRT hält sich bei der Bearbeitung, Bewertung und Veröffentlichung von Reports und Updates an die Prozesskette, die in der IEC 62443 gefordert wird.

„Bereits im Herbst 2018 wurde der Entwicklungsprozess für Produkte bei Phoenix Contact nach der Norm IEC 62443-4-1 zertifiziert. Damit ist Secure-by-Design bei uns fester Bestandteil bei der Entwicklung eines Security-Produktes“ hebt Roland Bent, CTO Phoenix Contact, die Maßnahmen im Unternehmen hervor. „Der nächste konsequente Schritt ist nun auch getan. Mit der jetzt erfolgten Zertifizierung wird bestätigt, dass unser Branchen-Marketmanagement sichere Automatisierungslösungen für unsere Kunden, entsprechend der Norm IEC 62443-2-4, entwickeln und umsetzen kann.“

Cyber Security ist in jeder Industrie relevant

Egal ob Hersteller oder Betreiber, Industrie oder kritische Infrastruktur – das Thema Cyber Security ist für

alle wichtig. Die Welt der Automatisierungstechnik wächst immer stärker mit der Welt der IT zusammen. Anlagengrenzen verschwimmen, die Menge der verfügbaren Daten steigt und der Austausch von Daten und Informationen wächst konsequent an. Diese zunehmende Vernetzung und Anbindung industrieller Steuerungs- und Automatisierungssysteme (ICS) an das Internet sorgt auch dafür, dass diese zunehmend Cyber-Angriffen ausgesetzt sind.

Die Fernwirktechnik ist ein wesentlicher Bestandteil der Automatisierung wasserwirtschaftlicher Anlagen. In Zuge der Digitalisierung bieten Ethernet-basierte Lösungen vielfältige Vorteile, beinhalten andererseits jedoch einige Herausforderungen. Via Ethernet werden oftmals Daten mit den Außenbauwerken ausgetauscht. Allerdings kann die Ethernet-basierte Vernetzung ebenfalls eingesetzt werden, um die Verfügbarkeit der Technik erheblich zu beeinflussen. Fast jeden Tag berichten die Medien von Angriffen mit Schadsoftware und deren gravierenden Folgen. Die Digitalisierung der Prozesse muss also unbedingt mit einer guten Strategie zur Umsetzung der IT-Sicherheit einhergehen.

Energieversorgung und Netzsteuerung sind Teil der Kritischen Infrastrukturen (KRITIS) in Deutschland. Fehlen Strom und Gas, kommt das öffentliche Leben innerhalb kürzester Zeit zum Erliegen und lebensnotwendige Dienstleistungen können nicht mehr erbracht werden. Die Funktionsfähigkeit der Energieversorgung ist von einer intakten Informations- und Kommunikationstechnologie abhängig. Dies macht IT-Sicherheit in der Energiebranche essentiell.

IEC 62443

Die Norm IEC 62443 ist eine Serie von Dokumenten und befasst sich mit der IT-Sicherheit sogenannter **Industrial Automation and Control Systems (IACS)**. Der Begriff IACS steht dabei für alle Bestandteile, wie Systeme, Komponenten und Prozesse, die für den sicheren Betrieb einer automatisierten Produktionsanlage erforderlich sind. Durch ihre spezifische Ausrichtung auf den Industriebereich setzt sich die IEC 62443 auch markant von der ISO 27001 ab, welche sich eher mit klassischen IT-Systemen beschäftigt.