Wago präsentiert Cloud Data Control

Neben den IoT-Controllern PFC100 und PFC200 erweitert Wago (www.wago.com) sein digitales Leistungsportfolio mit Wago Cloud Data Control. Die Lösung stellt das Bindeglied zwischen den Elementen der realen und der digitalen Welt dar. Dabei spielt einerseits die dezentrale Datenerfassung und zentrale Datenbereitstellung von der Feldebene bis in die Cloud und andererseits der standortunabhängige Zugriff auf aktuelle Daten eine entscheidende Rolle.

Bild: Wago

Wago Cloud Data Control verwaltet und überwacht alle Wago-Controller PFC sowie deren Applikationen und Daten. Ein Webportal dient dem Anwender als Bedienoberfläche für den Clouddienst, der bei Microsoft Azure gehostet wird. Über diesen hat er Zugriff auf Funktionen, wie Projekt-, Controller- und Benutzerverwaltung oder Controller-Status-Monitoring, Alarmfunktionen und E-Mail-Benachrichtigungen. Auf einem Dashboard lassen sich Texte, Tabellen, Diagramme, Zeigerelemente und Kommando-Buttons bedienen. Bei anwendungsspezifischen Lösungen kommt die Rest- oder OPC-UA-Schnittstelle zum Einsatz.

Angriff auf die Sicherheitssteuerung Triconex von Schneider Electric mit der Malware Triton

Nach Stuxnet und Industroyer hat mit Triton Mitte Dezember 2017 zum dritten Mal ein Hacker-Angriff auf eine industrielle Steuerung stattgefunden. Zum ersten Mal war jedoch eine Sicherheitssteuerung betroffen, die Triconex von Schneider Electric.

Nach Angaben des Spezialisten für datengestützte Sicherheit „FireEye“ (www.fireeye.com) versuchten die Cyber-Kriminellen, die Controller der Sicherheitssteuerung über einen Remote-Zugang einer Workstation neu zu programmieren. Als eine Gültigkeitsprüfung eines Anwendungscodes zwischen zwei redundanten Prozessoren scheiterte, fuhr die Sicherheitssteuerung die Anlage sicher herunter. Bedingt durch diesen Vorfall wurde die komplette Anlage analysiert.

Das eindeutige Ziel war, den Industrieanlagen, der Umwelt oder der Produktion zu schaden. Da die Angreifer die Malware „Triton“ eingesetzt haben, kurz nachdem sie Zugang zur Sicherheitssteuerung Triconex erhalten hatten, deutet darauf hin, dass sie die Schadsoftware vorher getestet haben müssen, was den Zugang zu spezieller Hard- und Software erfordert. Triton wurde speziell dafür entwickelt, um mit dem proprietären Kommunikationsprotokoll „TriStation“ zu interagieren.

Nach einer Meldung von Reuters haben sich weder „FireEye“ noch Schneider Electric zum Unternehmen, zur Branche oder zur Region des Angriffs geäußert. Das Cyber-Security-Unternehmen Dragos gab an, dass das Ziel „ein Unternehmen im Mittleren Osten“ gewesen sei. Laut Aussage von „CyberX“, einem anderen Cyber-Security-Spezialisten, ist das Opfer in Saudi-Arabien beheimatet.

Andy Kling, Director of Cybersecurity and Architecture bei Schneider Electric, unterstreicht in seinem Statement zu dem Angriff: „Wir wollen darauf hinweisen, dass das Ziel des Angriffs die Anlage bzw. der Anwender war. Obwohl Triton entwickelt wurde, um mit unseren Produkten zu interagieren, war dies der Fall, weil genau diese Produkte an diesem Ort in dieser Anlage verwendet wurden. Die Schadsoftware hat sich keine inhärente Schwachstelle in den Produkten von Schneider Electric zunutze gemacht.“

Cloudlösung für den Mittelstand

Als Hersteller von Industrietechnologien hat GE (www.ge.com/digital) die cloudbasierte IIoT-Plattform Predix für die Digitalisierung in der Industrie sowie zugehörige Technologien entwickelt. Die Plattform bietet Unternehmen standardisierte Möglichkeiten, um Innovationen zu realisieren. Entwickler können damit benötigte Applikationen auf Basis von Internet-Technologien (kurz: Apps) schnell erstellen, dabei Fehlerquellen minimieren und „Best Practices“ entwickeln sowie leicht austauschen.

„In Deutschland setzen wir für die Realisierung von Anwendungsprojekten im Mittelstand auf Partner wie Videc“, betont Simone Hessel, Head of Marketing GE Digital Europe. Die Predix-Cloud basiert auf einer globalen, sicheren Cloudinfrastruktur, die für industrielle Anwendungen optimiert ist und regulatorische Anforderungen erfüllt. Laut S. Hessel nutzt Predix die AWS-Cloud und Microsoft Azure, die beide in Deutschland gehostet werden. Die Predix-Cloud läuft in Deutschland und die Nutzungsrechte der Daten sind eindeutig geklärt. Die Plattform Predix funktioniert wie ein wiederverwendbares Baukastenprinzip. Die Verantwortlichen können Arbeiten besser verteilen, das Risiko von Kosten- und Terminüberschreitungen vermindern und Erstinvestitionen zukunftssicher gestalten.

Partnerschaft für den Mittelstand: Videc-Geschäftsführer Dieter Barelmann und Simone Hessel, Head of Marketing GE Digital Europe