Unsere Hard- und Softwareprodukte so zu gestalten, dass sie es unseren Kunden und den Anwendern ihrer Maschinen und Anlagen leicht machen, diese Ziele einzuhalten – und gleichzeitig ermöglichen, von den Vorteilen des IIoT zu profitieren –, ist ein wesentlicher Bestandteil unserer Produktstrategie.

Stefan Schönegger, Leiter Geschäftsbereich Controls bei B&R

CYBERSECURITY – KEIN LUXUS, SONDERN NOTWENDIGKEIT

Cybersecurity bei B&R als strategisches Unternehmens- und Entwicklungsziel: Die Flexibilisierung der Produktion braucht eine Vernetzung von Maschinen und Anlagen im Industrial Internet of Things und ihre Verbindung zur Informationstechnik (IT). Das öffnet auf allen Ebenen der Automationspyramide Angriffspunkte für unbefugte Zugriffe und gefährdet dadurch die Verfügbarkeit der Produktionsmittel. Im Zeitalter von Industrie 4.0 ist Cybersecurity daher kein Luxus, sondern Notwendigkeit. Bei B&R ist sie Teil einer weitreichenden unternehmensweiten Strategie, die Cybersecurity Officer Robert Fuchs und Stefan Schönegger, Leiter Geschäftsbereich Controls, im Interview erläutern. **Das Gespräch führte Ing. Peter Kemptner, x-technik**

Maschinen und Anlagen arbeiten längst nicht mehr isoliert abseits der IT, sondern sind mit dieser verbunden. Sie erhalten aus MES-Systemen Produktionsaufträge und aus CAM-Systemen automatisch aus den Produktdaten generierte Maschinenprogramme und liefern Betriebsdaten zurück. Ihre Steuerungs- und Automatisierungssysteme kommunizieren miteinander ebenso wie mit übergeordneten, oft standortübergreifend agierenden Leit- und Informationssystemen. Ihre Instandhaltung ist auf die Übertragung von Meldungen in externe Netze und von Fernzugriffen für Diagnose und Wartung angewiesen. Allein im Jahr 2022 wurden mehr als 600 Ransomware-Angriffe auf Industrieanlagen registriert. Dazu kommen schädliche Handlungen aufgrund unbefugter Zugriffe, die von eigenen Mitarbeitern auch ohne böse Absicht ausgeführt wurden. Das macht es nötig, Maschinen und Anlagen bestmöglich vor Bedrohungen zu schützen. Dabei unterstützt B&R seine Kunden durch Steuerungs- und Automatisierungssysteme, deren Entwicklung zertifiziert nach der Normenreihe IEC 62443 zur IT-Sicherheit für industrielle Kommunikationsnetze erfolgt.

Der B&R Site Manager sichert unter anderem OPC UA und Automation Studio Fernwartungszugriffe zielgerichtet und mit individuell einstellbarer Verschlüsselungstechnologie ab.

B&R nimmt seine Verantwortung für die OT-Sicherheit in der Lieferkette ernst. Die Zertifizierung nach IEC 62443-4-1 unterstreicht die Fähigkeit des Unternehmens, Kunden und Anwender bei der Identifizierung und Bewältigung von Sicherheitsrisiken zu unterstützen.

Robert Fuchs, Cybersecurity Officer bei B&R

Herr Schönegger, wie definiert B&R Cybersecurity?

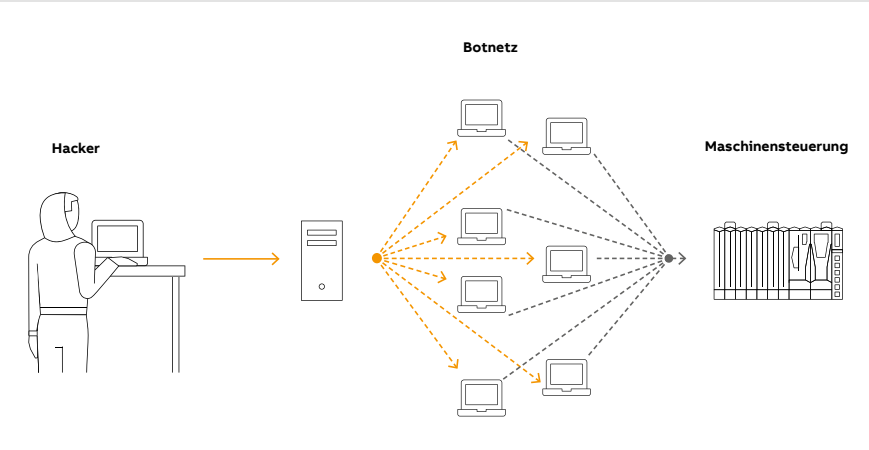
Cybersecurity ist für uns ein strategisches Unternehmensziel. Um es klar herauszustellen: Bei Cybersecurity unterscheiden wir einerseits Maßnahmen, die dem Selbstschutz dienen und andererseits solche, die wir zum Schutz unserer Kunden unternehmen. Im Zusammenhang mit Industrieanlagen dient Cybersecurity dem Schutz vor unbefugtem Zugriff und Angriffen von außen, um den Erhalt von Vertraulichkeit, Unversehrtheit und Verfügbarkeit der Steuerungs- und Automatisierungssysteme zu gewährleisten. Unsere Hard- und Softwareprodukte so zu gestalten, dass sie es unseren Kunden und den Anwendern ihrer Maschinen und Anlagen erleichtern, diese Ziele einzuhalten – und gleichzeitig ermöglichen, von den Vorteilen des IIoT zu profitieren –, ist ein wesentlicher Bestandteil unserer Produktstrategie.

Herr Fuchs, wie sorgen Sie als Cybersecurity Officer für die Umsetzung dieser Strategie?

Meine Rolle bei B&R ist, die Umsetzung der IEC 62443 Teile 4-1 und 4-2 nachhaltig zu betreuen und darauf zu achten, dass die Security-Zugewinne bei den einzelnen B&R-Produkten für unsere Kunden zugänglich gestaltet sind. Die IEC 62443-Normenreihe definiert eine Supply Chain Security (Lieferkettensicherheit). Dadurch geben wir Anwendern die nötigen Werkzeuge an die Hand, um normkonforme Maschinen und Anlagen zu entwickeln und betreiben. Ein sicherer Produktentwicklungsprozess (Secure Development Lifecycle) und Produkt-Security-Eigenschaften, deren z. B. Anwendung dokumentiert und modernen Security-Tests unterzogen wurde, tragen zur Supply Chain Security bei.

Nicht alle Leser kennen die IEC 62443. Wie definiert die Norm die produktbezogene Cybersecurity?

Die IEC 62443 ist keine rein technische Norm. Die internationale Normenreihe ist in verschiedene Bereiche unterteilt und beschreibt auch prozessorale Aspekte der industriellen Cybersecurity. Sie legt für Betreiber, Integratoren und Hersteller Anforderungen fest, deren Erfüllung durch Vermeidung und Behandlung von Sicherheitsrisiken >>



Bei einer DDoS-Attacke (Distributed-Denial-of-Service) verteilt ein Hacker seine Angriffsprogramme auf ein Botnetz und **kann durch eine gezielte Attacke eine Maschinensteuerung lahmlegen**.

In der strategischen Ausrichtung von B&R spielt Cybersecurity eine zentrale Rolle. Im Februar 2023 wurde der gesamte **Entwicklungsprozess des B&R-Echtzeitbetriebssystems Automation Runtime nach IEC 62443-4-1 zertifiziert**.

bei ihren jeweiligen Tätigkeiten zu einem hohen Maß an Cybersecurity führt. Für uns besonders relevant ist Teil 4-1 „Components and Requirements", der die Anforderungen an Prozesse der Produktentwicklung von Komponenten einer Automatisierungslösung beschreibt. Teil 4-1 der Norm legt fest, wie ein sicherer Entwicklungsprozess für Produkte auszusehen hat. Er umfasst das Management der Entwicklung, die Definition von Security-Anforderungen, das Design von Security-Lösungen, die sichere Entwicklung, das Testen von Sicherheitseigenschaften, den Umgang mit Sicherheitslücken, das Erstellen und Veröffentlichen von Updates sowie die Dokumentation der Security-Eigenschaften.

Herr Schönegger, wie weit reicht die Konformität von B&R mit der IEC 62443?

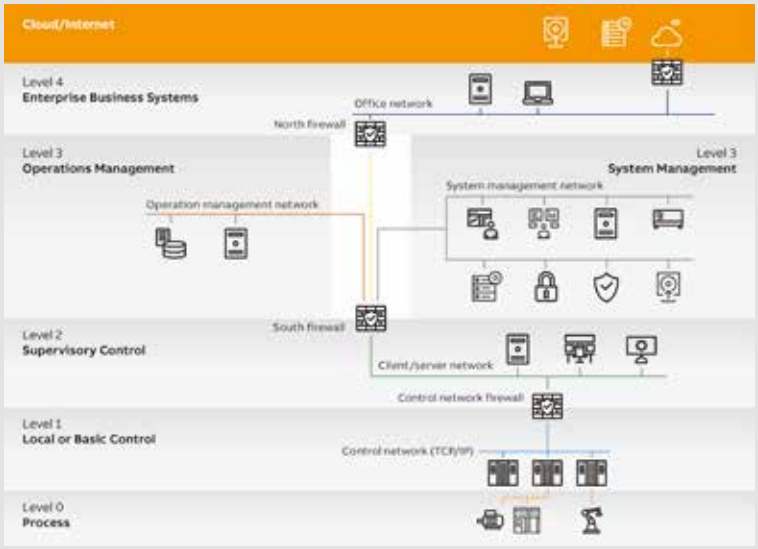
Im Februar 2023 wurde der gesamte Entwicklungsprozess des B&R-Echtzeitbetriebssystems Automation Runtime nach einem Audit durch den TÜV Rheinland nach IEC 62443-4-1 zertifiziert. Das betrifft sämtliche Phasen des Software-Produktlebenszyklus, von der Spezifikation über Design, Entwicklung und Test bis hin zur Wartung. Wir betrachten die Zertifizierung als zentralen Meilenstein in der strategischen Ausrichtung, Cybersecurity weiter im Produktportfolio zu verankern. Diese Strategie betrifft nicht nur die Gestaltung unserer Softwareprodukte, sondern alles, was mit dem Identifizieren und Bewältigen von Sicherheitsrisiken zu tun hat. Teil unseres modernen Schwachstellenmanagements ist beispielsweise, auf mögliche Sicherheitslücken, die wir nicht sofort technisch schließen können, explizit hinzuweisen und mögliche Maßnahmen zur Risikominimierung aufzuzeigen. Das tun wir mit voller Transparenz, indem wir auf der B&R-Website für Entwickler und Anwender stets aktuelle, genaue Beschreibungen der bestehenden Schwachstellen sowie Lösungsvorschläge bereitstellen.

Herr Fuchs, welche technischen Vorkehrungen in B&R-Produkten tragen konkret zu höherer Sicherheit im Sinn von Security bei?

Nun, das ist ein ganzer Themenkomplex. Es gibt keine einzelne Lösung für die Bekämpfung von Angriffen auf die verteilten Elemente von Steuerungssystemen. Wir begegnen dieser Herausforderung mit dem sogenannten Defense-in-Depth-Prinzip. Dabei gibt es eine Vielzahl von Maßnahmen auf unterschiedlichen Ebenen. Dieses Maßnahmenbündel findet sich in der Infrastruktur vor Ort wieder und erstreckt sich über die Maschine bis hin in die einzelnen Komponenten. Bei den Infrastrukturmaßnahmen beschreiben wir beispielsweise Schutzmaßnahmen in einer Referenzarchitektur, welche an die Automatisierungspyramide angelehnt ist. Unsere Entwicklungsumgebung Automation Studio enthält sehr viele kleine, in der Summe jedoch sehr wirksame Maßnahmen zur Abwehr von Bedrohungen auf der Maschinenebene. Diese umfassen z. B. das „Hardening" mit einer integrierten Firewall. Wir setzen auf das Kommunikationsprotokoll OPC UA, das inhärent über sehr gute Schutzmechanismen verfügt und haben einige potenziell anfällige Kommunikationskanäle stillgelegt. Dazu kommt die vollständige Protokollverschlüsselung für HTTP-Verbindungen wie webbasierte Visualisierung mit mapp View, Microsoft Active Directory-Anbindungen und weitere Dienste.

Benutzerauthentifizierung gab es ja im Automation Studio auch bisher schon, oder?

Natürlich, und sie bietet ein Beispiel dafür, wie auch ganz kleine Maßnahmen zu einem veritablen Plus an Sicherheit führen können. In der Vergangenheit wurden unsere



B&R beschreibt Security-Maßnahmen in der Infrastruktur vor Ort in einer Referenzarchitektur, welche an die Automatisierungspyramide angelehnt ist.

Software und unsere Geräte mit voreingestellten optionalen Netzwerkdiensten ausgeliefert. Die hat nur deaktiviert, wer dieses Verhalten bewusst ändern wollte. Kontinuierlich setzen wir auf sichere Standardeinstellungen (Secure by Default), sodass der Anwender gezwungen ist, etwas zu ändern. Wer optionale Netzwerkdienste verwenden möchte, muss dies schon bewusst tun. Dazu kommt der Einsatz von asymmetrischer Verschlüsselung mit dem Austausch digitaler Zertifikate für das Signieren und Verifizieren von Daten und für die Authentifizierung von Geräten und Benutzern. Das hilft zuverlässig, die Unversehrtheit von Daten zu gewährleisten.

Sind nicht auch Edge Device im IIoT Angriffspunkte?

Ja, denn beim Edge Computing werden große Datenmengen möglichst nahe an der Datenquelle erfasst, komprimiert und aggregiert, um dann an übergeordnete Systeme weitergeschickt zu werden. Als Bindeglied zwischen der echtzeitgetriebenen Maschinen- und Prozessebene (OT = Operational Technology) und der IT bieten wir Edge-Geräte an. Sie haben integrierte Firewalls und kommunizieren verschlüsselt über OPC UA.

Als heikler Fall für die Security gilt die Fernwartung. Wie sehen Ihre Lösungen für diesen Bereich aus?

Genau diesen Anwendungsfall deckt der SiteManager ab, den wir seit einigen Jahren anbieten. Dieses Edge Device mit interner Firewall ist als Hard- oder Softwarevariante zur Anbindung von LAN, WLAN oder Mobilfunk verfügbar. Um Sicherheitskonflikte mit werksseitigen Firewalls zu vermeiden, läuft die Kommunikation in das Internet über Firewall-verträgliche, verschlüsselte Web-Protokolle.

Herr Schönegger, wie gut werden Ihre Angebote zur Cybersecurity vom Markt angenommen?

Das hängt ein wenig von der Branche ab. Energie und Infrastruktur oder die Automobilindustrie sind da weiter als der Werkzeugmaschinenbau oder die Kunststoffindustrie. Allerdings sorgt schon allein die Vorschriftenlage dafür, dass Security nicht länger optional ist, sondern Standard. Die IEC 62443 als Basisnorm fließt aktuell in die Schiffsklassifizierung DNV-GL und in die neue Maschinenrichtlinie ein. Auch der EU Cyber Resilience Act, die Cybersicherheits-Richtlinie NIS 2.0 und die chinesische Rechtsvorschrift GB40050 übernehmen sinngemäß ihre Regelungen. Es ist daher keine Frage der individuellen Akzeptanz, sondern des Bestrebens unserer Kunden, ihr Risiko durch Verwendung passender Produkte zu begrenzen. Genauso machen sie es seit vielen Jahren im Bereich der funktionalen Sicherheit.

Wie sieht es mit der Verfügbarkeit dieser technischen Sicherheitseigenschaften aus, wie ist die Zukunftsperspektive?

Die genannten Maßnahmen sind in Einführung und werden sukzessive in neuen Versionen von Automation Runtime verfügbar. Die TÜV-Zertifizierung erstreckt sich aktuell ausschließlich über die Organisationseinheit um das Kernprodukt Automation Runtime. Wir arbeiten aber natürlich daran, diese Zertifizierung auf alle Bereiche unseres Unternehmens und unseres Produktportfolios auszudehnen.

Vielen Dank für das Gespräch.

www.br-automation.com