CYBER-SICHERHEIT FÜR DIE INDUSTRIE

WARUM SCADA NICHT MEHR VERWENDET WERDEN SOLLTE?

Khobeib Benboubaker
Industry Business Line Manager, Stormshield

Heute werden die Industriesysteme immer mehr digital gesteuert, was sie Cyberangriffen aussetzt. Angesichts des steigenden Risikos ist die Kenntnis der Grundlagen der Cyber-Sicherheit für die Industrie sowie der diesbezüglichen technischen Begriffe eine notwendige Voraussetzung, um die Gefahren effizient angehen zu können.

SCADA, ICS, DCS, HMI, PLC ... Alleine hinter dem Begriff OT (*Operational Technology* – im Gegensatz zu IT, *Information Technology*) verstecken sich im Industriejargon zahlreiche Bezeichnungen, deren Auslegung je nach Branche und Unternehmen unterschiedlich ist. „*Selbst der Begriff OT ist komplex und uneinheitlich*“, erklärt Vincent Riondet, Verantwortlicher der Teams für Cyber-Sicherheits-Projekte und -Dienstleistungen bei Schneider Electric France. „*Das macht ihn zum Waisenkind des traditionellen Informationssystems*“. Diese Begriffe werden häufig falsch übersetzt oder auf verschiedene Art und Weise erfasst, weshalb diese Industriebegriffe zu Verwirrung führen können, insbesondere innerhalb der Teams für IT-Sicherheit. Um die Industrieanlagen zu schützen, ist eine gute Kenntnis ihrer Funktionsweise und der sie bezeichnenden Begriffe entscheidend, um die angemessenen Maßnahmen ergreifen zu können. Dies gilt umso mehr, wenn man einen laufenden Cyberangriff parieren muss.

WORUM HANDELT ES SICH BEI SCADA?

Der Begriff SCADA (*Supervisory Control And Data Acquisition*) hat im Industriejargon einen zentralen Platz eingenommen. Seine Definition wird jedoch in Abhängigkeit der Regionen, jedoch auch der Berufe, unterschiedlich ausgelegt. SCADA kann eine auf einem PC installierte Software bezeichnen, mit der Daten erhoben werden, oder ein System zur allgemeinen Überwachung. Ein erster Versuch, der bereits Probleme bereitet.

„Es ist in der Tat die SCADA-Terminologie, die bei den IT-Akteuren am meisten für Verwirrung sorgt", so Vincent Riodet. *„Ein CISO versteht somit unter dem Begriff SCADA die gesamte operative Technologie." „Für einen Automatiker wiederum bezeichnet SCADA das System, mit dem man eine große Anzahl an Daten erheben und verarbeiten kann. Es handelt sich dabei um eine Überwachungssoftware. Für Leute, die nicht im Feld der Automatik tätig sind, kann der Begriff, im falschen Sprachgebrauch, jegliches System zur Industriekontrolle bezeichnen*", ergänzt Fabien Miquet, Product & Solution Security Officer bei Siemens. Desgleichen wird ein Integrator mit SCADA alles bezeichnen, was in einem Industriesystem installiert ist, bis hin zu den Controllern.

„Eine Person aus der IT versteht nicht das Gleiche unter SCADA wie eine Person aus der OT."

Vincent Riondet, Verantwortlicher der Teams für Cyber-Sicherheits-Projekte und -Dienstleistungen bei Schneider Electric France

In der Praxis wird SCADA in Europa generell als System zur Fernverwaltung und Fernmessung verstanden, das in Echtzeit kommuniziert und zur Kontrolle der Anlagen verwendet wird. Auf der anderen Seite des Atlantik ist dies jedoch eine ganz andere Geschichte.

ICS, DCS, HMI, PLC: IM HERZEN DES INDUSTRIEJARGONS

In den USA wird der Begriff SCADA insbesondere mit einer breiteren Definition verwendet als in Europa, da er ein globales Überwachungssystem bezeichnet, das aus ICS, DCS, HMI und anderen PLC besteht.

Beim ICS (*Industrial Control System*) handelt es sich um Akronym, welches das gesamte Industriesystem umfasst. Sein Zweck ist es, alles zu kontrollieren, wodurch auch SCADA laut der europäischen Ansicht inbegriffen ist, und diese beiden Begriffe werden häufig durcheinandergebracht. *„Durch falschen Sprachgebrauch nennen Personen außerhalb der Automatik das ICS ein SCADA-System"*, erklärt Fabien Miquet. Als globales System wird es oftmals als Achillesferse der Cyber-Sicherheit für die Industrie angesehen, da seine Angriffsfläche, also inwiefern es dem Cyber-Risiko in Abhängigkeit seiner Größe ausgesetzt ist, von Natur aus umfassender ist.

„Durch falschen Sprachgebrauch nennen Personen außerhalb der Automatik das ICS ein SCADA-System."

Fabien Miquet, Product & Solution Security Officer Siemens

Neben ICS und SCADA wird auch der Begriff DCS (*Distributed Control System*) verwendet. Und mit den anderen beiden verwechselt. Dieses andere System ist vernetzt und ermöglicht die Vernetzung mehrerer Steuerungen oder kann sie sogar ersetzen, um komplexere Prozesse mit lokal verteilten Aufgaben zu verwalten.

Die Schnittstellen zwischen Mensch und Maschine (MMS oder HMI *für Human Machine Interface auf Englisch*) entsprechen wiederum Schnittstellen, mit denen der Benutzer sich mit einem System oder einer Steuerung verbinden kann. Hierbei handelt es sich um den Kommunikationskanal zwischen SCADA (der die Daten erhebt) und dem Menschen (der diese benötigt). In Frankreich wird dieser Begriff häufig mit SCADA verwechselt. „*Es ist schade, dass wir den Rest der Übersetzung weggelassen haben*", bedauert Vincent Riondet. „*Die Automatiker in Frankreich sprechen von SCADA eher nur, wenn sie sich auf die oberen Schichten der Prozessleitsysteme (die Überwachung und den Datenverlauf) beziehen. Auf europäischer Ebene bezieht man hier auch die Controller mit ein.*"

Ein anderer häufig verwendeter Begriff ist der PLC (*Programmable Logic Controller*), wobei es sich wiederum um ein System handelt, mit dem man autonome Steuerungen kontrollieren kann. Auf Deutsch spricht man von einer „*speicherprogrammierbaren Steuerung*" oder SPS. Können Sie noch folgen?

„*All diese Bereiche, IT, OT und Automatisierung, haben ihren eigenen Jargon. Wenn man sie alle mit SCADA bezeichnet, führt dies bei den Mitarbeitern zu Unverständnis. Und wenn man sich bei den technischen Begriffen nicht einig ist, führt dies wiederum zu Schwachstellen bei Angriffen*", legt Fabien Miquet mit einem gewissen Abstand dar.

WARUM ES SO WICHTIG IST, DEN INDUSTRIEJARGON ZU VERSTEHEN

Aus dieser Verwirrung entstehen gewisse **Cyber-Risiken der Industrie 4.0**. Denn wenn man sich ähnelnde Begriffe, die jedoch nicht dieselbe Funktion oder dieselben Ziele haben, falsch verwendet oder sie verwechselt, wird hierdurch die Aufgabe der Cyber-Sicherheit der Industriesysteme erschwert.Ohne hieraus ein „*Finde die Unterschiede*"-Spiel zu machen, kann man doch schnell die wichtigsten Unterschiede zwischen SCADA und DCS zusammenfassen, wobei es sich um einen echten Spannungsherd des Industriejargons handelt.

- Ein DCS ist auf die Prozesse ausgerichtet, wobei ein SCADA-System sich eher auf die Erhebung von Daten konzentriert;

- Ein DCS wird von Prozessen gesteuert, indem Sensoren, Controller, Einheiten oder Betätigungsgeräte verbunden werden, während ein SCADA-System von chemischen, physischen oder linearen Ereignissen gesteuert wird;

- Ein DCS ist stärker integriert und kann komplexere Handlungen vornehmen, während ein SCADA-System flexibler ist.

So können die Schwachstellen und Cyber-Gefahren eines jeden bestmöglich antizipiert werden. Und im Voraus angegangen werden, um das gesamte Industriesystem effizienter zu schützen.

DIE CYBER-SICHERHEIT FÜR DIE INDUSTRIE HEUTE GARANTIEREN

Für die Unternehmen bergen die Produktionseinheiten das **wichtigste Cyber-Risiko. Denn ein Cyberangriff kann sie stören,** beschädigen oder sogar lahmlegen und somit zu schwerwiegenden finanziellen Verlusten führen, manchmal sogar auch Auswirkungen auf das Personal und die Umwelt haben. Eine Schwachstelle, die insbesondere darauf zurückzuführen ist, dass die OT-Welt sich nicht in demselben Tempo weiterentwickelt wie die IT.

„Die OT wandelt sich weniger schnell als die IT. Die Cyber-Sicherheit muss sich an die Industrie anpassen, nicht andersherum. Da lässt sich nichts machen. Man muss manchmal bei bestehenden Elementen einen Reverse-Engineering-Ansatz verfolgen, um die bestmöglichen Lösungen anbieten zu können", so die Analyse von Franck Bourguet, Vice President Engineering von Stormshield.

Denn ein Produktionsgerät soll mehrere Jahrzehnte halten und dabei durchgehend in Betrieb sein. Dies erschwert die Aktualisierungen neben der Wartung, die weit im Voraus geplant sind, um sich so wenig wie möglich auf die Produktionsketten auszuwirken. In der Vergangenheit funktionierte die OT darüber hinaus ohne Internet und war somit den direkt aus dem Internet stammenden Gefahren nicht ausgesetzt. Mit der digitalen Revolution und der Automatisierung werden die Fabriken nun jedoch vernetzt und müssen sich nun den Cyber-Risiken stellen.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security).

www.stormshield.com

Version 1.1 - Copyright Stormshield 2020