OT-Security ist von Anfang an einzuplanen

Neue Regelwerke haben Auswirkungen auf das OT-Netzwerk

Für Maschinenbauer und Anlagenbetreiber wird Security ein immer wichtigeres Thema. Normen wie die IEC 62443 stellen u.a. Anforderungen an die Systemsicherheit und Sicherheitsstufen. Ziel ist es, die Cyber-Resilience der Industrie zu stärken, gerade auch auf Operative Technology (OT)-Ebene. Denn immer öfter wird diese von Angriffen auf die IT-Ebene quasi als „Beifang" in Mitleidenschaft gezogen. Gleichzeitig sollte sie aber auch vor direkten Angriffen, die im Produktionsumfeld stattfinden, geschützt werden. Sicherheit ist also ein Thema, das nicht nur die einzelnen Anlagenteile, sondern gerade auch das eingesetzte Kommunikationsnetzwerk betrifft.

Anlagen bestehen in der automatisierten Fertigung oder der Prozessindustrie aus zahlreichen Einzelmaschinen. Das Management initialisiert Digitalisierungsprojekte wie z.B. Prozessoptimierung, Steigerung der Prozesstransparenz, Energiemanagement usw. Dadurch wandeln sich die Anforderungen an die Netzwerk-Kommunikation und deren Sicherheit. Nach aktuellem Stand wird die IEC 62443, Teil 3-3(„Anforderungen an die Systemsicherheit und Sicherheitsstufen" über den Anhang III 1.1.9 auch in die Maschinenverordnung eingehen und die Voraussetzungen für eine sichere Kommunikation schaffen. Unabhänig davon sind schon jetzt die Verordnungen der Richtlinie hilfreiche Vorgaben, um Securtiy in einem OT-Netzwerk zu gewährleisten. Es ist davon auszugehen, dass schon bald von Anlagenbauern und -betreibern mehr Netwerk-Know-how gerfordert wird. Oder sie holen sich, wie auch beim Maschinenbau, externe Expertise ins Haus.

Security-Konzepte

OT-Security ist nichts, was man nach Fertigstellung einer Anlage einfach noch „überstülpen" könnte. Vielmehr betrifft das Thema die Anlage bei jeder verbauten Komponente und bis in die Tiefe der physikalischen Netzwerkstruktur. Cyber-Security muss daher von Anfang an eingeplant werden. Dazu sieht die IEC 62443 verschiedene Security-Konzepte vor, die die eingesetzte Hardware und Systeme ebenso betreffen wie Prozesse im Unternehmen und den Reifegrad der Organisation, sprich das Verständnis der Mitarbeiter für die vorhandenen Prozesse und das Wissen darum, was im jeweiligen Problemfall zu tun ist.

Die Netzwerkexperten von Indu-Sol beschäftigen sich seit ihrer Gründung vor gut zwanzig Jahren mit der Zuverlässigkeit von industriellen Netzwerken. Rogèr Costa, Leiter Marketing bei Indu-Sol, erklärt: „Ein Netzwerk, das aus welchen Gründen auch immer nicht zuverlässig funktioniert, hat stets auch Einfluss auf die Sicherheit der gesamten Anlage. Wir können mit unseren Tools transparent machen, was im Netz-

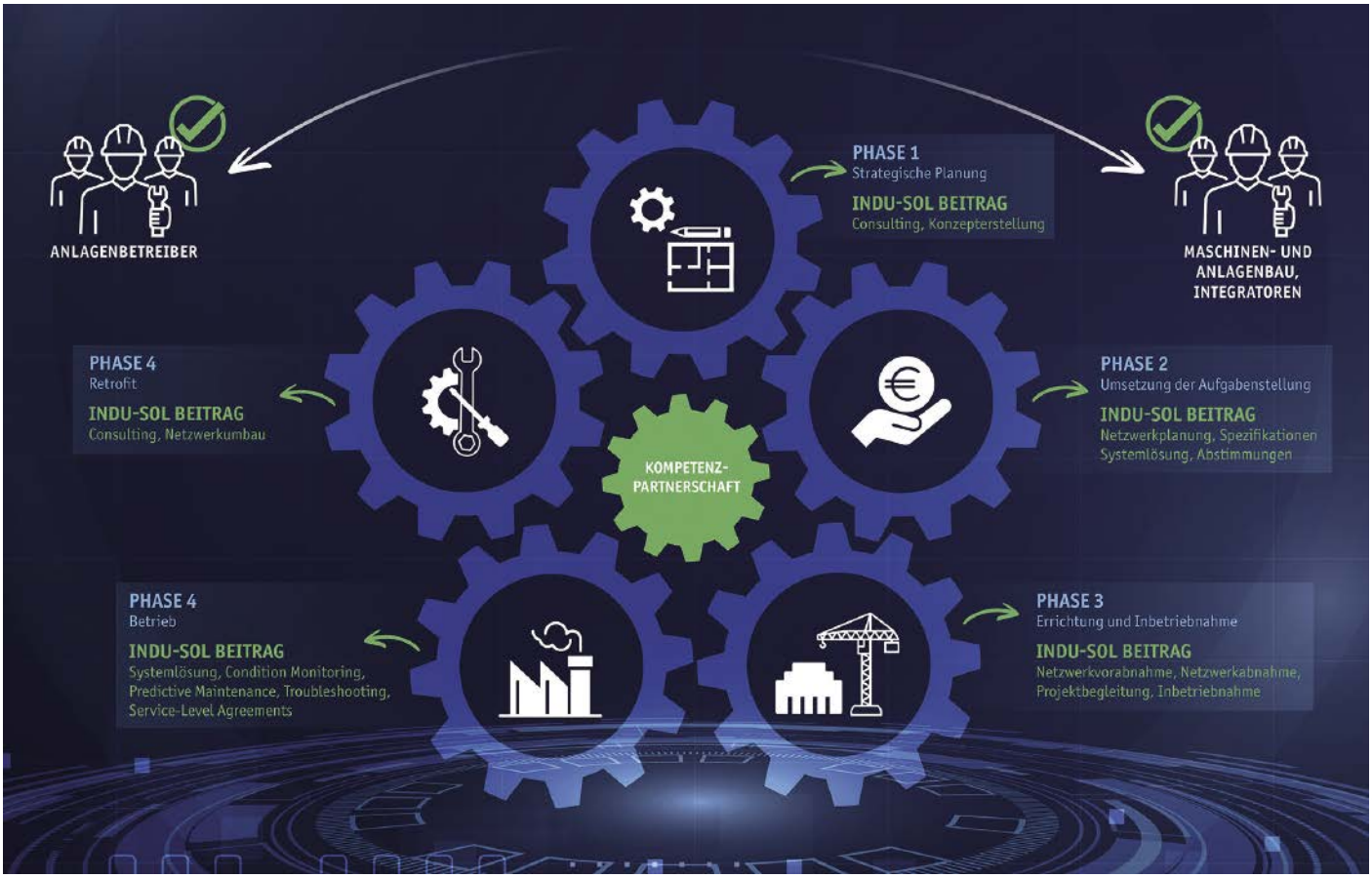


Abb. 1: Tools und Strategien für Cyber-Security betreffen den ganzen Lebenszyklus einer Anlage.

werk los ist. Gerade auch in Bezug auf Security von Netzwerken können wir Anlagenbauer und -betreiber in den Bereichen Hardware und Systeme sowie bei dem Reifegrad der Organisation über entsprechende System-Schulungen unterstützen."

Netzwerk im Anlagen-Lebenszyklus

Wer OT-Security in Anlagen einplant, sollte das also auch beim Netzwerk tun. Das ist aber ein komplexes Unterfangen, das nicht einfach so nebenbei erledigt werden kann. Es bräuchte sowohl bei der Anlagenplanung als auch im späteren Betrieb einen Experten für Netzwerktechnik. Das ist aber in der Regel aus finanzieller Sicht nicht machbar und im Zuge des Fachkräftemangels sind gut ausgebildete Mitarbeiter für die Netzwerktechnik schwer aufzutreiben. Hier kann es sinnvoll sein, bereits ab der ersten Phase des Anlagenlebenszyklus das Thema Netzwerk an externe Dienstleister auszulagern (Abb. 1). Das bringt den zusätzlichen Vorteil, dass es bei der Übergabe der fertiggestellten Anlage von Anlagenbauer an den Anlagenbetreiber nicht zu einem Zuständigkeitswechsel bei der Netzwerktechnik kommt.

Netzwerkexperten können bereits in der Phase der strategischen Planung beratend unterstützen. In der Phase von Umsetzung und Aufgabenstellung übernehmen sie dann die Netzwerkplanung. Bei der Einrichtung und Inbetriebnahme kümmern sie sich um die Netzwerkabnahme, im laufenden Betrieb über entsprechende Service-Level Agreements um Condition Monitoring und Predictive Maintenance. Wo es in Anlagen zum Retrofit kommt, stehen sie ebenfalls beratend zur Seite und helfen beim Netzwerkumbau. Für all diese Tätigkeiten braucht es dreierlei: Know-how, die passende Hardware sowie Services passend zur jeweiligen Lebensphase der Anlage.

Tools mit integrierter Expertise

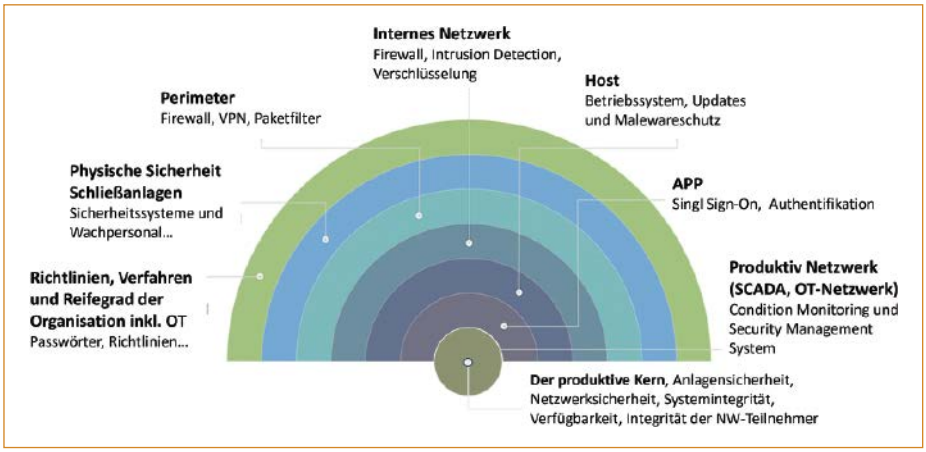
Die Zeiten, in denen OT-Netzwerke noch vom Rest der Welt unabhängige Inseln waren, sind weitestgehend vorüber. Zu groß die Vorteile, die sich durch konvergente Netzwerke und direkten Zugriff auf die Smart-Sensor-Daten der Maschinen und Anlagen ergeben. Zunehmend sind intern daher OT-Netzwerke mit der IT-Ebene verknüpft. Costa sagt: „Das heißt dann aber auch, dass jede Komponente, in der eine CPU verbaut ist, angreifbar ist. Damit ist das Thema OT-Security stark mit der eingesetzten Hardware verwoben. Der Clou ist, dass unsere Lösungen, die sich in den vergangenen Jahren für den zuverlässigen Betrieb von Netzwerken mit dem Schwerpunkt auf Predictive Maintenance bewährt haben, auch zur Überwachung der Netzwerksicherheit eignen. Wir sprechen daher inzwischen bei unserem System von einem CM&SM (Abb. 2), einem Condition Monitoring & Security Management System."

© Indu-Sol

Abb. 2: Condition Monitoring und Security Management System (CM&SM) für Anlagen und OT-Netzwerke mit Profinet und Ethernet/IP.

Um OT-Security zu gewährleisten, stellt die IEC 62443-3-3 verschiedene Anforderungen, die letzten Endes die Voraussetzung für das Verteidigungsprinzip „Defense in Depth" (Abb. 3) liefern. Die Forderungen beziehen sich auf Identifizierung bzw. Authentifizierung, Nutzungskontrolle, Systemintegrität, Vertraulichkeit der Daten, eingeschränkten Datenfluss, rechtzeitige Reaktion auf Ereignisse sowie die Verfügbarkeit der Ressourcen. Jede dieser sieben Anforderungen braucht verschiedene Tools bzw. Maßnahmen, um sie zu realisieren. Die verschiedenen Lösungen von Indu-Sol können in ganz unterschiedlichen Bereichen helfen. Dazu einige Beispiele: Ein initialer Topologie-Scan zur Identifizierung bzw. Authentifizierung von OT-Netzwerken sowie ein wiederkehrender Scan lassen sich bspw. mit Condition Monitoring & Security Management System realisieren und verwalten. Die Tools der Netzwerkexperten prüfen die Datenkommunikation auf unerwünschte Veränderungen, setzen Verschlüsselungsmethoden zur sicheren Datenübertragung ein, segmentieren aus Sicherheitsgründen einzelne Netzwerkbereiche, sorgen für kontinuierliche Datenüberwachung und automatisierte Alarmierung oder helfen bei der Sicherung und Wiederherstellung von Gerätekonfigurationen.

„Die Liste der Anforderungen und wie sich diese mit unserem System erfüllen lassen ist lang", erläutert Costa. „Ein Trend ist aber klar: Mit den Forderungen der IEC 62443 und bald auch mit der neuen Maschinenverordnung liegt künftig ein stärkerer Schwerpunkt auf der OT-Sicherheit industrieller Kommunikationsnetze. Dafür braucht es Lösungen in Form von Komponenten, unterstützenden Systemen aber auch Fachkräfte oder Dienstleister mit dem entsprechenden Know-how. Wir bringen dieses Know-how im Rahmen einer OT-Kompetenzpartnerschaft auf Augenhöhe ein. Die gute Nachricht ist, dass hier das Rad nicht neu erfunden werden muss, sondern bewährte Lösungen parat stehen, um sich diesen neuen Anforderungen souverän zu stellen."



© Indu-Sol

Abb. 3: Exkurs: ISA/IEC 62443 – die Schichten von Defense in Depth aus Sicht der OT.

Autoren: Denise Fritzsche, Marketing bei Indu-Sol, Nora Crocoll, Redaktionsbüro Stutensee

Kontakt:
Indu-Sol GmbH
Schmölln
Denise Fritzsche
Tel.: +49 34491/580-0
info@indu-sol.com
www.indu-sol.com