„Security by Design ist nicht sinnvoll“

Die große Verschmelzung von IT und OT bringt sowohl für die Funktionale Sicherheit als auch die Cybersecurity enorme Herausforderungen mit sich. Technologien wie MTP, NOA und APL lassen den Komplexitätsgrad außerdem zusätzlich ansteigen. Im Interview legen Thomas Königstein, Chief Information Security Officer bei HIMA, und Peter Sieber, Vice President Strategic Marketing, dar, wie eine moderne Automation Security aussehen muss und weshalb Security by Design dabei keine Rolle spielt.

Herr Königstein und Herr Sieber, durch die stetige Verschmelzung von IT und OT lassen sich Safety und Security nicht mehr getrennt voneinander betrachten. Welche Konsequenzen hat das für Sie?
Peter Sieber: Grundsätzlich gilt für uns der folgende Grundsatz: Ohne Security gibt es keine Funktionale Sicherheit. Schließlich sind heute fast alle Sicherheitssysteme in übergeordnete Leitsystemkonzepte eingebunden. Safety und Security müssen daher Hand in Hand gehen. HIMA ist deswegen seit Ende der 1990er Jahre auch im Security-Bereich aktiv.

Thomas Königstein: Die Auswirkungen dieser Verschmelzung spiegelt ja schon allein die Tatsache wider, dass Sie mit Peter Sieber, einem Safety-Experten, und mir, dem Chief Information Security Officer von HIMA dieses Interview führen. Interdisziplinäres Arbeiten ist in diesem Bereich einfach sehr wichtig, denn aus unserer Sicht ist Security ein Teamsport, der auf die Expertise unterschiedlicher Gewerke angewiesen ist.

Sieber: Das hat auch HIMA gemerkt und dahinter steckt auch die Motivation des Unternehmens, nicht mehr nur in Produkten zu denken, sondern sich auf ganzheitliche Lösungen zu konzentrieren. Wer heute ein sicheres und secures Produkt entwickelt, hat wirtschaftlich bestenfalls nur den zweitbesten Lösungsweg gewählt. Es müssen vielmehr systemisch alle relevanten Aspekte der Safety und Security abgedeckt werden, um auch ökonomisch gut dazustehen.

Was sind denn die wesentlichen Grundlagen eines modernen ganzheitlichen Security-Konzepts?
Königstein: Als allererstes muss man sich darüber klar werden, was ich konkret schützen will, welche Ziele Angreifende wählen könnten. Darüber hinaus ist es wichtig zu wissen, welchen Schaden sie verursachen könnten und wie schnell ich auf eine Attacke reagieren kann. Grundsätzlich gibt es darüber hinaus dann aber kaum ein Standard-Security-Konzept, dass alles abdeckt. Mit Basis-Methoden ist vielleicht ein Security-Level von 80 % zu erreichen. Alles weitere kann nur mit individuellen Lösungen realisiert werden, wobei natürlich eine einhundertprozentige Absicherung nicht möglich ist. Und weil eben mit dem großen Standard-Hammer schon viele Probleme erschlagen werden können, tut sich da ein gewisses Spannungsfeld auf. Denn jedes Unternehmen muss für sich entscheiden wie viel Investment über eine Basis-Security hinaus sinnvoll und wirtschaftlich ist.

Sieber: Die Normierung versucht hier Abhilfe zu schaffen. Ich arbeite seit vielen Jahren an der IEC 62443 aktiv mit und ein spezielles Team befasst sich aktuell damit, ein Konzept zu erarbeiten, mit dem Security und Funktionale Sicherheit koordiniert werden können. Dieser Technical Report 63069 ist 2019 erstmals veröffentlicht worden und kann im Webstore der IEC auch erworben werden. Die NAMUR hat mit der NE 153 (Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme, Anm. d. Red.), die ich mitverfasst habe, auch entsprechend ein Automation-Security-Konzept entworfen.

Was aber bereits sieben Jahre alt ist. Ist eine Überarbeitung notwendig?
Sieber: Nein, meiner Meinung nach spricht die NE 153 viele Punkte an, die auch heute noch relevant sind. Der einzige Aspekt, den ich heute etwas anders darstellen würde, betrifft das Konzept der *Security by Design*. Vor sieben Jahren haben wir noch von Automatisierungsprodukten geträumt, die gleichzeitig sicher und secure sein können. Wir bei HIMA haben uns von dem Gedanken jedoch verabschiedet.

Warum?
Sieber: Weil wir es aktuell nicht für ökonomisch sinnvoll halten, alle für potenzielle Security-Anforderungen notwendigen Funktionen in ein Sicherheitssystem zu implementieren. Es wird dadurch so komplex, dass die notwendige funktionale Sicherheit des Geräts nicht mehr gewährleistet werden kann.

Königstein: Der Grundgedanke „More secure by design“ wäre sicherlich der realistischere Ansatz. Das aktuell diskutierte *Security by Design* hat den Anschein einer selbsterfüllenden Prophezeiung. Insbesondere reden wir von einer Bedrohungslage, die nicht berechenbar ist, weil wir Angreifenden gegenüberstehen, die unendlich viele Möglichkeiten haben. Insofern halte ich diesen absoluten Ansatz nicht für zielführend, sondern spreche mich eher für eine Art Security-Baseline im Design aus.

Aber wie hoch muss diese Baseline denn sein? Wann bin ich ausreichend abgesichert?
Sieber: Das kommt immer auf das jeweilige Unternehmen an. Fakt ist: Heute müssen wir nicht nur davon ausgehen,

Peter Sieber befasst sich bereits seit fast 40 Jahren mit der Funktionalen Sicherheit und seit mehr als 15 Jahren auch mit der Security.

Für Thomas Königsstein ist Security by Design kein Konzept für die Zukunft, sondern mehr eine sich selbst erfüllende Prophezeiung.

dass ein Angriff auf ein betriebliches Automatisierungssystem jederzeit möglich ist, sondern auch, dass dieses System versagt. Eben deswegen gibt es die davon unabhängigen Sicherheitssysteme, die dafür sorgen, dass die Anlagen in einen sicheren Zustand überführt werden können und Mensch und Umwelt keinen Schaden nehmen. Aus unserer Sicht ist für die Security-Betrachtung daher im Grunde genommen derselbe Maßstab anzulegen.

Das müssen Sie genauer erklären.

Sieber: Die Sicherheitssysteme dienen der Risikoreduzierung im Anlagenbetrieb. In unserer beinahe vollständig digitalisierten Welt von heute müssen wir neben den bekannten Risiken wie z. B. technischem Versagen, unbekannten Verfahren oder menschlichen Fehlern auch die Risiken aus der IT und OT berücksichtigen und die Systeme so konzipieren, dass sie auch nach erfolgreichen Cyberangriffen in den sicheren Zustand überführt werden können. Das gelingt uns mit dem HIMA Security Environment für Funktionale Sicherheit.

Königstein: In dieser IT-Umgebung befinden sich neben den Sicherheitssystemen selbst auch die zugehörigen Engineering-, Bedien- und Beobachtungssysteme, die dort alle gleichermaßen geschützt sind. Dieser Bereich wird nun von der kritischen Umgebung in angemessenem Maße abgeschottet.

Was bedeutet hier „angemessen“?

Sieber: Übertragen auf die Safety ist das Ziel immer SIL 3. Das bedeutet im Klartext pro 1.000 Betriebsjahre ein einziges gefährliches Versagen. Zum Vergleich: die „normalen“ Automatisierungssysteme in der Verfahrenstechnik erreichen fast SIL 1, was von einem solchen Vorfall pro Jahr ausgeht. Von den Sicherheitssystemen wird also erwartet, dass sie 1.000-mal sicherer sind als die gewöhnliche Automatisierungstechnik. Die Herausforderung ist es jetzt, diesen Anspruch von der Safety auf die Security zu übertragen.

Was muss dafür getan werden?

Sieber: Wir müssen auf jeden Fall deutlich schärfere Maßstäbe anlegen, als es die Kolleginnen und Kollegen tun, die sich mit der Prozessleittechnik beschäftigen. Das eben angesprochene Security Environment ist ein erster Schritt in diese Richtung, weil es die wichtigen Systeme in einer Art Kokon einschließt, wo diese hohen Sicherheitsanforderungen in die Tat umgesetzt werden können.

Nun werden auch in der Prozessindustrie Anlagen in Zukunft stark modular aufgebaut. Welche Herausforderungen bringt z. B. das MTP für ein solches Security Environment mit sich?

Königstein: Wir müssen analog zu den Produktions-Modulen eben auch Safety- und Security-Module liefern, die entsprechend vorgeprüft und im Bedarfsfall individuell angeordnet werden können. Gemeinsam mit entsprechenden Prüfprogrammen bekommen Anwendende so die Möglichkeit, im Falle einer Änderung flexibel zu reagieren.

Sieber: Das wäre der konventionelle Weg, aber es gibt noch einen anderen, bei dem nicht die Funktionalitäten der einzelnen Devices einer Anlage im Vordergrund stehen. Vielmehr wird der Prozess, der in dem Gehäuse stattfindet und dessen Integrität in den Fokus gerückt.

Sie gucken quasi in den Rührkessel hinein und nicht mehr von außen drauf?

Sieber: Genau, denn wenn der Kessel seine Form verändert, ist es zu spät. Wir betrachten also die chemischen Reaktionen, die dort stattfinden, bilden die dazugehörigen thermodynamischen Funktionen ab und lassen dann ein Programm im Sicherheitssystem laufen. Dieses Programm überwacht schließlich, ob alles im grünen Bereich ist oder ob eingegriffen werden muss. Das ist zwar recht aufwendig, bietet aber gerade für den Einsatz von MTPs einen spannenden Ansatz, weil wir in Bezug auf die Safety und Security unabhängiger von der Instrumentierung werden.

Königstein: Wir als klassischer Lieferant wissen nämlich nicht zwangsläufig, wie der Betrieb der kompletten Anlage aussieht. Im Umkehrschluss bedeutet das bezogen auf die Modularisierung wieder eine enge interdisziplinäre Arbeit, die aufgrund eben der komplexen Prozesse notwendig ist. Das Verstehen der Prozesse wird gerade bei der Modularisierung elementar wichtig, eben um auch skalierbare Lösungen anbieten zu können. Unser neues Customer Solutions Center ist ein wichtiger Schritt in diese Richtung.

In der Prozessindustrie werden neben dem MTP auch NOA und APL in absehbarer Zeit marktreif. Wie betrachten Sie diese Technologien bezogen auf die Security?

Sieber: Meiner Meinung nach liegen Fluch und Segen hier nah beieinander. NOA z. B. ist wunderbar, um die traditio-

„Ohne Security gibt es keine Funktionale Sicherheit. Safety und Security müssen Hand in Hand gehen."

nelle Sichtweise der Automatisierungshierarchie in eine digitalisierte Welt überführen kann. Auch auf jeder Ebene dieser Hierarchie Daten abzugreifen und sie Auswertungen zuzuführen ist prinzipiell kein Problem, aber wir müssen dafür das Security-Thema in den Griff kriegen. Mit der Datendiode, dem *Verification of Request*, ist dies schon bereits vorgedacht worden. Bei der Umsetzung setzen wir auf die genua GmbH, die für unsere Lösungen sehr taugliche Datendioden zur Verfügung stellt.

Königstein: Wenn wir über APL sprechen, dann kommt es jetzt auf die Komponentenhersteller an, auch APL-fähige Geräte auf den Markt zu bringen. Wir von unserer Seite sind startklar und haben die entsprechenden Software-Funktionen veröffentlicht. Die Herausforderung liegt hier bei den mit APL enorm steigenden Datenmengen, die kommuniziert werden können. Schließlich ist 4…20mA und HART immer noch oft das Maß aller Dinge. In Zukunft können jedoch bis zu 10 Mbit pro Sekunde übertragen werden.

Diese Datenwelle will erstmal verarbeitet werden.
Sieber: Deshalb gibt es ja bereits den Ansatz, die für die Automatisierungsfunktionen unwichtigen Datenströme nach NOA-Vorbild am Automatisierungssystem vorbeizuführen. Ich bin hier noch unsicher, weil wir ja trotzdem noch die sichere von der nicht-sicheren Kommunikation trennen müssen. Auch hier könnte eine Art Datendiode helfen, die Ströme so zu richten, dass keine funktionalen Probleme zu erwarten sind.

Königstein: Dennoch bieten APL und NOA große Chancen, um den Wissenstransfer zwischen IT und OT voranzutreiben und damit eben auch die Verschmelzung der Domänen sowie die Digitalisierungsgeschwindigkeit zu beschleunigen. Dazu muss man wissen, dass das NOA-Konzept z. B. in der IT nicht unbedingt etwas Neues ist. Gerade im Geheimschutzbereich gibt es ähnliche Technologien mit geheimen und nicht geheimen Netzwerken seit Jahrzehnten.

Blicken wir noch etwas weiter in die Zukunft und in Richtung autonomer Anlagen, die sich durch KI und Machine Learning selbst optimieren. Wie muss sich die Security darauf vorbereiten?
Königstein: Am Ende des Tages ist es ehrlich gesagt schwer vorstellbar, dass wir eine Art künstliche Logik schaffen, die Effizienzsteigerungen und Dynamisierungen erreicht, die bezogen auf die Security mit SIL-3-Niveau vergleichbar sind. Es gibt in der Security und der Safety grundlegende fundamentale Regeln, die sich in Kenngrößen wie eben den SIL-Levels niederschlägt. Und solange eine künstliche Logik die notwendige Baseline an Security-Anforderungen erfüllt, werden wir sie einsetzen können. Kurz gesagt: es wird eine Art natürliche Barriere für die KI-basierte Security geben.

Sieber: Genauso wie es auch in Zukunft immer noch bestimmte Regeln geben wird, nach denen die produzierenden Anlagen, die wir absichern werden, funktionieren. Wie diese Regeln aussehen und umgesetzt werden weiß ich nicht, aber auch in 20 Jahren wird ein Behälter aus den Fugen gehen oder eben nicht. Dabei spielt es auch keine Rolle, was in dem Behälter passiert, wie er automatisiert wird oder ob ein kognitives System draufschaut. Es geht darum, die Risiken zu kennen und zu beherrschen. Diese Grundpfeiler werden sich nicht verändern.

ZUR PERSON

Peter Sieber
Seit seinem Abschluss als Ingenieur ist Peter Sieber seit über 37 Jahre in der Prozessautomatisierung tätig und hatte verschiedene Führungspositionen bei führenden internationalen Prozessautomatisierungsunternehmen inne. Nach seinem Einstieg bei HIMA als Sales Manager im Jahr 2013 wurde er 2016 zum Vice President Norms & Standards und Vice President Region China ernannt. Seit Juni 2022 ist er Vice President Strategic Marketing.

Thomas Königstein
Seit über 15 Jahren ist Thomas Königstein im Bereich der IT-Security tätig. Seit 2019 ist er Chief Information Security Officer (CISO) der HIMA Gruppe.