Zielgerichtete IT/OT-Integration: Sicherheit und Industrie 4.0 Hand in Hand

Rudolf Preuss

Wenn es um Cybersecurity in der Produktionsumgebung (OT-Cybersecurity) geht, so prallen zwei Welten aufeinander. Auf der einen Seite die IT, die auf alle Herausforderungen mit einer Materialschlacht von Hardwarekomponenten, Firewalls und softwarebasierten Security-Lösungen antwortet, auf der anderen Seite die OT-Verantwortlichen, deren Fokus auf dem stabilen Betrieb und der funktionalen Sicherheit der Produktionsanlagen liegt.

Dabei liegt es auf der Hand, dass die zielgerichtete Integration von IT- und OT-Systemen Vorteile mit sich bringt, denn durch Kooperation und Austausch von Wissen aus diesen beiden Schlüsselbereichen eröffnen sich nicht nur Wege zu einem höheren Sicherheitsniveau, sondern auch klare Antworten auf die drängenden Fragen bei der Umsetzung von Industrie 4.0. Dieser Vision vom Zusammenwachsen von IT und OT stehen mit dem Silodenken und dem Beharrungsvermögen großer Organisationen Hürden entgegen, die zuvor beseitigt werden müssen.

Kooperation von IT und OT

VINCI-Energies strebt durch das Zusammenspiel mit den Konzernmarken Actemium als Systemintegrator für Industrieautomatisierung und Axians als ICT-Dienstleister eine enge Kooperation von IT und OT an. Diese beiden unabhängigen Organisationseinheiten zeichnen sich durch ein spezifisches Leistungsprofil aus und besitzen auf ihrem jeweiligen Gebiet großes Know-how. Durch die Aufteilung in eine Vielzahl einzelner Business Units, die einen hohen Grad an Autonomie besitzen, wird eine hohe Flexibilität gewährleistet.

Im Bereich OT-Cybersecurity arbeiten Actemium und Axians als Partner für die Industrie eng zusammen. Das Heben von Synergieeffekten erfolgt dabei jedoch nicht automatisch, sondern erfordert strategische Planung, gute Vorbereitung und Beseitigung von Hindernissen, die der Realisierung des Geplanten entgegenstehen.

Herausforderungen bei der OT-Security

Als ein mögliches Hindernis ist die kulturelle Differenz zwischen den IT- und OT-Teams zu nennen. Das Erfolgsrezept der IT ist die schnelle Transformation. Der Kern des Geschäftsmodells besteht überwiegend aus Serviceleistungen des laufenden Betriebs, wie Infrastructure-as-a-Service (IaaS) oder Software-as-a-Service (SaaS), deren Fakturierung den operativen Kosten zugeordnet werden (Opex). Demgegenüber ist die Kernkompetenz der OT die Stabilität und Zuverlässigkeit der Anlagen, die mit hohem Investitionsaufwand langfristige Erträge generieren sollen (Capex). Diese unterschiedlichen Ansätze können bei der Zusammenarbeit zu Missverständnissen und Kommunikationsproblemen führen.

Eine Schwierigkeit bilden die Wissenssilos, die sich über Jahre hinweg gebildet haben. Jede Gruppe hat ihr eigenes spezialisiertes Wissen, das meist ungern mit anderen Bereichen geteilt wird. Der Austausch von Informationen und Best Practices zwischen den Business Units ist jedoch erforderlich, um eine umfassende Sicherheitsstrategie für die Kundenprojekte zu entwickeln.

Als bedeutender Aspekt ist die unterschiedliche Nutzung gleicher Technologien in IT und OT zu nennen. Beispielsweise wurde zu Anfang Virtualisierung in der OT als beliebtes Instrument genutzt, Entwicklungsumgebungen von Projekten einzufrieren und gegen die sich verändernde IT-Umgebung abzuschirmen. Inzwischen sind virtualisierte Leitsysteme der Industriestandard.

Des Weiteren unterscheiden sich IT und OT in ihrem Umgang mit Zeit. In der OT herrschen strenge Echtzeitanforderungen. Hier kann einerseits die Einhaltung eines Zeittakts von wenigen Millisekunden entscheidend sein, andererseits dürfen Updates und Retrofit-Maßnahmen auf das nächste oder übernächste Wartungsfenster verschoben werden, da derartige Aktualisierungen der Systeme komplex und kostspielig sein können. In der IT-Welt sind schnelle Sicherheits-Patches bekannter „Schwachstellen“ unumgänglich und Updates erfolgen teilweise mehrmals am Tag, andererseits fallen Schwankungen im Bereich von Millisekunden kaum ins Gewicht.

Zu erwähnen bleibt auch, dass viele OT-Systeme zu einer Zeit entwickelt wurden, in der IT-Sicherheit keine Priorität darstellte. Aus diesem Grund bedarf es spezieller Ansätze, um Legacy-Systeme sicher in die IT-Umgebung einzubinden.

Abbildung 1: Ein physikalisches Modell mit drei gekoppelten Tanks. Angesteuert von Prozessleitsystemen drei unterschiedlicher Hersteller (Siemens - PCS Neo, B&R - Aprol, Schneider Electric - ProLeit) ist dieser Demonstrator ein Showcase, um Konzepte der OT-Cybersecurity zu verproben.

Wissensaustausch und Kommunikation

Maßgeblich für die erfolgreiche Umsetzung von Projekten im Umfeld von IT und OT ist ein offener Wissensaustausch sowie eine effektive Kommunikation der handelnden Personen. Diese beiden Elemente sind entscheidend, um das bereits genannte Silodenken zu überwinden und eine Kultur der Zusammenarbeit und des Austauschs zu fördern. Hilfreich sind hierbei moderne Kommunikationstechnologien. Tools wie Intranet-Plattformen, Chat-Systeme und Projektmanagement-Software ermöglichen es Teams, in Echtzeit zusammenzuarbeiten und Informationen effizient zu teilen.

Ebenso sind in diesem Kontext regelmäßige Meetings wichtig, um Projekte zu besprechen und gemeinsame Ziele zu definieren. In Zeiten von Home-Office können Präsenzschulungen und Workshops helfen, das notwendige Vertrauen (Trust) zwischen den Akteuren aufzubauen, damit Kooperation gelingt. Auch dies ist ein wichtiger Baustein, um das Bewusstsein für die Bedeutung der IT-OT-Integration zu schärfen und notwendige Fähigkeiten zu vermitteln. So einfach es klingen mag: Die Kaffeemaschine hat sich als eines der effektivsten Instrumente des Wissens-Managements erwiesen.

Voraussetzung für das Verstehen von Sachverhalten ist die Entwicklung einer gemeinsamen Sprache mit einem einheitlichen Vokabular und verbindlichen Regeln. Ein Beispiel für die Notwendigkeit einer gemeinsamen Sprachregelung illustriert der folgende Ausschnitt aus einem Angebotstext von Axians:

„Aufbau virtuelle Umgebung in der OT DMZ mit Erstellung FDS“:

Der Begriff war manchen Kollegen unbekannt. Erst der voll ausformulierte Text brachte hier Klarheit:

„Der Aufbau einer virtuellen Umgebung in der Operational Technology (OT) Demilitarisierten Zone (DMZ) mit der Erstellung einer Funktionsdesignspezifikation (FDS).“

Ein weiterer Baustein der Kooperation ist eine Kultur, in der konstruktives Feedback gefördert und geschätzt wird, damit sich kontinuierliche Verbesserungen entwickeln können. Als eine wichtige Erkenntnis der Ingenieurswissenschaften gilt, dass man Fehler nicht selbst machen muss, sondern von den Fehlern und dem daraus entstandenen Wissen anderer lernen kann.

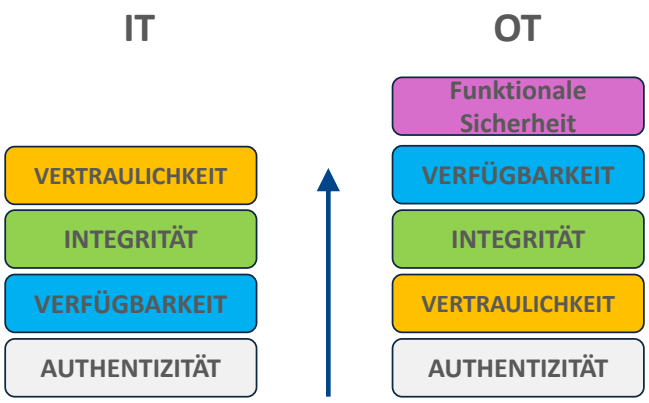

Abbildung 3: Ziele und Prioritäten von IT + OT-Sicherheit im Überblick.

Bei VINCI-Energies existiert hierfür eine zentrale, für die Mitarbeiterinnen und Mitarbeiter zugängliche Wissensdatenbank, in der Informationen, Best Practices und Lösungen gespeichert werden. Für den Themenbereich der OT-Cybersecurity wurde das ganze „Kochbuch“ genannt und für die Kommunikation mit den Kunden als „Haute Cuisine der IT-OT-Sicherheit“ präsentiert. Mit einem Augenzwinkern kann man auf diese Weise die schiere Menge der Einzelmaßnahmen strukturieren und in bearbeitbare Leistungspakete aufteilen.

Die Digitalschmiede als Ort des Lernens und Experimentierens

Mit der Digitalschmiede in Frankfurt am Main besitzt VINCI-Energies einen Ort, an dem Neues ausprobiert und entwickelt werden kann. Diese Einrichtung steht den Business Units und deren Kunden offen. Ihre Aufgabe ist es, den digitalen Wandel zu beschleunigen und nachhaltig zu verankern. Mit ihren verschiedenen physikalischen Modellen und Demonstratoren spielt die Digitalschmiede eine entscheidende Rolle bei der Überwindung des Silodenkens und dient zugleich als praktische Plattform, auf denen IT- und OT-Experten gemeinsam an realen Problemen arbeiten und neue Lösungen entwickeln können. Ein Beispiel für einen Demonstrator in der Digitalschmiede ist in Abbildung 1 zu sehen.

Der OT-Hackathon in der Digitalschmiede

Ganz im Zeichen des Lernens und Experimentierens stand der OT-Hackathon 2024 in der Digitalschmiede (10.-12.07.2024) mit dem Thema „OT-Cybersecurity“. Die konkrete Aufgabe der Teilnehmenden bestand aus der Erarbeitung des OT-Cybersecurity-Showcase für die Digitalschmiede. Mitgedacht war die interne Fortbildung der Mitarbeitenden von VINCI-Energies sowie die Vernetzung und der Austausch mit Systemherstellern und Lieferanten.

Drei gemischte Teams aus den Konzernmarken Actemium und Axians bekamen die Aufgabe, innerhalb von 48 Stunden ihre Konzepte und Lösungsvorschläge zu erarbeiten. Die Hersteller der Prozessleitsysteme B&R, Schneider Electric und Siemens, Fortinet als Netzwerkausrüster und die Firma softScheck als Spezialist für Security-Tests standen den Teams während des Hackathon als Berater zur Seite. Darüber hinaus stellten die Hersteller zusammen mit den Vertretern der Digitalschmiede auch die sachkundige Jury, welcher die Ergebnisse in einem jeweils 20-minütigen Pitch mit anschließender Q&A Session präsentiert wurden.

Ergebnisse des Hackathon

Der Hackathon brachte IT- und OT-Fachleute in einem informellen, kreativen Umfeld zusammen. Die Teilnehmenden hatten die Gelegenheit, ihre Erfahrungen auszutauschen und die Herausforderungen des jeweils anderen besser zu verstehen. Diese offene Kommunikation half, Vorurteile abzubauen und eine Grundlage für die zukünftige Zusammenarbeit zu schaffen. Im Vordergrund stand dabei die vertiefte Debatte zwischen IT und OT über die unterschiedliche Priorisierung von Zielen und zugleich deren „richtige“ technische Umsetzung.

Der grundlegende Unterschied zwischen IT und OT wurde bei der Setzung von Prioritäten innerhalb der CIA-Triade (Confidentiality, Integrity, Availability) deutlich. In der IT-Welt liegt der Fokus traditionell auf der Vertraulichkeit. Datenlecks und unautorisierte Zuggriffe können schwerwiegende Folgen haben, von Identitätsdiebstahl bis hin zu finanziellen Verlusten. Daher wird großer Wert auf Verschlüsselungstechniken und Zugriffskontrollen gelegt, um sicherzustellen, dass sensible Informationen geschützt bleiben.

Im Gegensatz dazu steht in der OT, insbesondere in kritischen Infrastrukturen, die Verfügbarkeit im Vordergrund. Ein Ausfall von Steuerungssystemen kann zu unmittelbaren physischen Schäden und Gefahren für das menschliche Leben führen. Deshalb sind Redundanzen und resiliente Netzwerke von höchster Bedeutung, um die kontinuierliche Funktion der Betriebstechnologien zu gewährleisten.

Die Integrität der Daten und Systeme ist sowohl in der IT als auch in der OT von zentraler Bedeutung, allerdings mit unterschiedlichen Implikationen. In der IT geht es darum, Manipulationen zu verhindern, die zu falschen Entscheidungen führen könnten. In der OT hingegen kann eine Beeinträchtigung der Integrität direkte Auswirkungen auf die physische Welt haben, wie etwa die Fehlfunktion von Maschinen oder Anlagen. Damit wird die funktionale Sicherheit als übergeordnetes Ziel der OT deutlich.

Ein während des Hackathon von IT und OT gemeinsam erarbeitetes Ergebnis war die Ergänzung der CIA-Triade um den Topic Authentizität in seinen unterschiedlichen Ausprägungen wie MFA etc. und deren mögliche technische Umsetzung.

Die Herausforderung besteht darin, ein Gleichgewicht zwischen diesen Prioritäten zu finden. Die Integration von Wissen aus ICT und Automatisierungstechnik ermöglicht es, ein umfassendes Sicherheitskonzept zu entwickeln, das die spezifischen Anforderungen beider Bereiche berücksichtigt. Dieser integrative Ansatz ist der Schlüssel, um nicht nur ein höheres Sicherheitsniveau zu erreichen, sondern auch die Vision von Industrie 4.0 zu realisieren.

Am Ende des Hackathon stand fest, dass das Thema OT-Cybersecurity Fachkräfte benötigt, die Domainwissen auf den Gebieten von IT und von OT besitzen. Die gute Nachricht hierzu: In fast allen Unternehmen sind diese „Superheldinnen“ und „Superhelden“ bereits vorhanden. Um deren Superkräfte zu entfalten, müssen sie nur miteinander ins Gespräch gebracht werden.

Rudolf Preuss
Koordinator IT/OT
Actemium Controlmatic West GmbH
54516 Wittlich