Chefsache: Automation Security

Automation Security - Sicherheit in Produktionsnetzen

Stuxnet hat die Automatisierer in aller Welt aufgerüttelt: Die Frage „Ist meine Produktion sicher?“ gewinnt eine neue Qualität. IT und Ingenieure können Lösungen liefern. Die Antwort auf die Sicherheitsfrage muss sich das Management erarbeiten.

Erwin Kruschitz, Vorstandsvorsitzender, Anapur

Angesichts einer schweren Bergtour denkt man beim Thema Sicherheit zuallererst an Seil und Haken. Analog dazu drängen sich „Firewall“ und „Virenscanner“ schnell in den Vordergrund, wenn es um Sicherheit von Produktionsnetzen und Automatisierungssystemen geht. Beides geht am Kern der Sache gründlich vorbei. Der Erfolg einer Bergexpedition basiert vornehmlich auf einer zuverlässigen Wetterprognose, einer detaillierten Routenplanung und einem trainierten, gesunden und kooperativen Team. Die Qualität des Seils ist wichtig. Der wahre Erfolgsfaktor besteht aber in der Einschätzung der Risiken (Wetterkapriolen, Lawinengefahr, Schwierigkeitsgrad der Wegstrecke, Versorgung mit Wasser). Basierend darauf wird der Abgleich zwischen den Risiken auf der einen Seite und den Sicherheitsmaßnahmen auf der anderen Seite durchgeführt. „Können“ und „Erfahrung“ sind dabei meist auf verschiedene Personen verteilt und müssen durch eine kompetente Leitung koordiniert werden. Mit der Sicherheit von Produktionssystemen verhält es sich sehr ähnlich.

Automation Security: aktuell wie noch nie

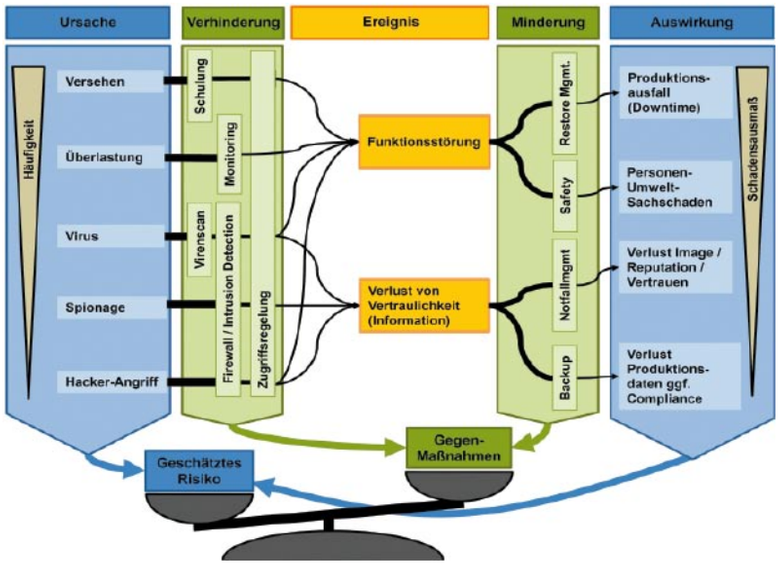
Ein Virus hat sich über ein Jahr lang unerkannt in Produktionsnetzen und Anlagensteuerungen festgesetzt. Virenscanner und Firewalls waren machtlos. Die Infektion erfolgte über Wechselmedien (USB-Stick). Nach der Erkennung des Virus dauerte es vier Monate, bis geklärt war, mit welchen konkreten Auswirkungen auf die Steuerung zu rechnen ist. Dass es nicht zu größeren Schäden gekommen ist, verdanken wir lediglich der „freiwilligen Selbstbeschränkung“ des Computerschädlings Stuxnet, der sich auf ganz spezielle Automatisierungsprodukte und Applikationen (Siemens S7-300, S7-400) fokussiert. Obwohl durch den Virus in Deutschland kein Schaden in Produktionsanlagen bekannt geworden ist, muss die Risikoeinschätzung verändert werden. Das Risiko, dass es zu einer Verletzung der Integrität des Steuerungsteils eines Automatisierungssystems kommt, wurde vor Stuxnet als sehr gering eingestuft. Stuxnet hat jetzt eindrucksvoll bewiesen, dass er nicht nur zu einer Störung, sondern darüber hinaus zu einer ganz gezielten Manipulation eines Prozesses fähig ist. So kann Stuxnet zum Beispiel über die Manipulation von Frequenzumformern Motordrehzahlen verändern.

Was ist zu tun?

Zunächst der rechtliche Aspekt: Risiko-Management ist nach KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) Aufgabe der Vorstände bzw. Geschäftsführer. Das ist auch weitgehend bekannt und wird bereits entsprechend adressiert. Auch Wirtschaftsprüfern ist das Thema Informationssicherheit vertraut. Allerdings konzentrierte man sich bis dato auf die Informationssicherheit in der Bürowelt. Die Produktionswelt unterscheidet sich in ihren Risiken, Anforderungen und den verwendeten Technologien jedoch sehr deutlich vom Office-Bereich.

„Können“ und „Erfahrung“ als Mittel gegen Risiken. Am Berg und in der Technik.

Will man im Produktionsbereich Sicherheit gemäß dem „Stand der Technik“ herstellen, stehen einige Normen und Regelwerke zur Verfügung. Alle Standards fordern den Aufbau einer „Sicherheits-Organisation“ (eines Management Systems). Dort sollen Verantwortlichkeiten und Prozedere festgelegt werden. Das Ziel dieses Management Systems ist die Aufrechterhaltung einer nachhaltigen Balance zwischen Risiken und Gegenmaßnahmen. Im Detail sind das: ISO270xx, das Grundschutzhandbuch des BSI (Bundesamtes für Sicherheit in der Informationstechnik), die IEC 62443/ISA99 und die VDI/VDE 2182. Dort, wo die Sicherheit von Personen und der Umwelt betroffen sind („Safety“), gilt auch die IEC61508/61511.



Automation Security ist erreicht, wenn sich organisatorische und technische Maßnahmen in Balance mit den Risiken befinden.

Worin bestehen die Risiken?

Die Grafik skizziert eine typische und generalisierte Risikolandschaft eines Produktionsbetriebs. Den blau dargestellten Risiken werden die grün dargestellten Barrieren gegenübergesetzt (Risikograd von oben nach unten abnehmend). Allgemein kann gesagt werden, dass Versehen (menschliche Fehler) als Schadensursache an der Spitze stehen. D.h.: Jeder Euro, der in Schulungen für Risiko-Analysen und Systemwiederherstellung investiert wird, bringt mehr Sicherheit als die Investition in Technologie (Virenscan und Firewalls). Das Risiko, das für die Personen und Umweltsicherheit (Safety) aus IT-Security Problemen entsteht, wird allgemein unterschätzt. Die organisatorische und gedankliche Trennung von Safety und Security wird heute fälschlicherweise mit der technologischen Trennung der Systeme argumentiert. Allerdings: Zufriedenstellend kann die Frage nach den Risiken und Schutzbarrieren letztendlich nur in einer Risiko-Analyse im Zusammenhang mit dem verfahrenstechnischen Prozess und der Betriebsorganisation beantwortet werden.

Warum ist Automation Security Chefsache?

Risiken einschätzen: Eine gute Analyse der Risiken ist das wichtigste Erfolgskriterium in der Automation-Security. Nur ein interdisziplinäres Team, geführt durch das Management, wird sicher feststellen, welches die kritischen Funktionen im Produktionsprozess sind und welche Informationen sensibel sind.

Zielvorgaben: Viele Entscheidungen im Automation-Security-Prozess bergen Zielkonflikte. Ein typisches Beispiel ist die Frage, wer auf welche Funktion bzw. Information Zugriff erhalten soll. Erhält der externe Dienstleister Zutritt oder Zugriff auf das Produktionssystem, dann ist eine schnellere Störungsbehebung denkbar (d.h., die Verfügbarkeit wird erhöht), aber der Kreis der Personen mit Zugriff auf sensible Informationen wird größer (d.h. Vertraulichkeit eingeschränkt).

Gegenmaßnahmen: In vielen Fällen gibt es für eine Bedrohung mehrere mögliche Gegenmaßnahmen. So könnten man für den Fall der Störung eines Teilsystems eine Redundanz für dieses System vorsehen (technische Lösung) oder die Bediener darauf schulen, den Prozess für die Zeit, die für die Wiederherstellung benötigt wird, von Hand zu fahren.

IT-Abteilung vs. Ingenieurabteilung: In den meisten Unternehmen gibt es eine Aufgabentrennung zwischen IT und Produktionstechnik. Für Automation Security haben beide eine Schlüsselrolle. Wer soll die Führung übernehmen?

Fazit

Automation Security ist Teamarbeit und muss frei von Abteilungsdünkeln funktionieren. Das „Können“ und die „Erfahrung“ der Beteiligten werden durch eine übergeordnete Führungsperson oder durch einen externen Koordinator zusammengeführt. Automation Security ist primär eine Organisations- und Managementaufgabe, die durch IT und Ingenieure unterstützt wird.

■ Kontakt:
Anapur AG, Ludwigshafen
Tel.: +49 621 595704 0
info@anapur.de
www.anapur.de

chemanager-online.com/tags/automation