Ein bisschen anfälliger als früher

Ist meine Anlage jetzt wirklich sicher?

„Mit der Anlagensicherheit beschäftigt man sich seit Jahren sehr intensiv. Auch GMP-Fragestellungen sind mittlerweile etabliert. Das Thema IT-Security ist in der Produktion Neuland. Bedingt durch den technologischen Fortschritt sowie durch neue Normen, ist dieses Feld für viele Firmen neu zu bestellen."
Erwin Kruschitz, Vorstand der anapur AG

Eigentlich ist alles ganz einfach. Die heutigen Produktionsnetze sind vernetzter und die Geräte vielfach Windows-basiert. Das bedeutet im Klartext: Alles ist ein bisschen anfälliger als früher. Erwin Kruschitz, Vorstand der anapur AG, überwacht diese modernen Systeme auf die Einhaltung von Good Manufacturing (GMP, GAMP) und Functional Safety Management (FSM) Richtlinien und sprach Klartext mit der IT&Production.

Wir unterscheiden in einem Betrieb erst einmal verschiedene Zonen: den Produktionsbereich mit Systemen wie HMI oder Engineering, Produktionsnahe IT, Unternehmens-IT und externe IT – und dazwischen schalten wir eine Firewall. Damit auch wirklich keine unerwünschten Rückwirkungen im Produktionsbereich vorkommen, schafft man eine sog. demilitarisierte Zone. Damit man auch tatsächlich merkt, wenn etwas nicht stimmt, überwacht man das ganze an den neuralgischen Stellen mit Intrusion Detection Systemen. Damit das Ganze noch irgendwie betrieben werden kann gibt's Security Policies, Trainingsprogramme und Incident Response Mechanismen usw. Die Frage, die bleibt, lautet: Ist meine Anlage jetzt sicher? Und wenn ja, wie sicher ist sie? Sehr sicher oder eher 'für unsere Zwecke reicht's' oder dominiert das Gefühl, 'ein schlimmer Virus könnte unsere Produktion lahm legen'? Also führt man ein Assessment durch.

IT&Production: Was ist Sicherheit für ein Unternehmen aus dem Umfeld Chemie, Pharma, LifeScience? Was gehört zu einem runden Konzept dazu?

Erwin Kruschitz: Sicherheit ist die Abwesenheit von nicht tolerierbarem Risiko. Ich muss zwei Dinge definieren können: Welches Risiko ist da? Und welches Risiko will ich tolerieren? Aus diesen Parametern kann ich dann Sicherheit ableiten oder den Grad der Sicherheit ableiten. Das ist einer der ersten Denkschritte, die zu tun sind – egal, ob wir über IT-Security oder Anlagensicherheit sprechen. Die Frage danach, was für ein Risikopotenzial existiert und welches Risikopotenzial ich bereit bin zu tolerieren, steht am Beginn eines Nachdenkens über Risiko und Sicherheit und ist möglicherweise auch eine der schwierigsten. Eine Antwort kann bspw. durch Firmenpolitik beeinflusst sein. Aktuell haben wir im Golf von Mexiko ein Problem. Da entsteht Bewusstsein, da entsteht Sensitivität. In so einer Phase wird man vielleicht dazu tendieren, weniger Risiko zu tolerieren. Die Antwort auf die Frage nach Sicherheit und Risiko ist in diesem Fall durch politische und gesellschaftspolitische Einflüsse geprägt.

IT&P: Die anapur AG betreut Projekte wie den Shut-Down für petrochemische Anlagen oder die Risikoanalyse für Automatisierungstechnik. Wie direkt ist aus Ihrer Sicht der Zusammenhang zwischen diesen Aspekten von Sicherheit und Informationstechnologie im Produktionsumfeld?

Kruschitz: Eine Pharma-Wirkstoffproduktion scheint von einer Gasförderanlage gedanklich recht weit entfernt zu sein. Das ist sie auch, wenn wir die Anlagen betrachten. Betrachten wir jedoch die Mechanismen: Wie analysiere ich Risiken? Wie gehe ich geordnet und geplanter Weise vor, um eine Risikoanalyse vorzunehmen und dann entspre-

chend Maßnahmen zu setzen? Wie bringe ich die organisatorischen Rahmenbedingungen auf die Reihe? Das ist der gemeinsame Nenner, und der unterscheidet sich eigentlich nicht davon, ob ich jetzt über IT-Risiken spreche, über Patientenrisiken, GMP-Risiken oder Anlagensicherheitsrisiken. Die Grundlagen, Methoden und Vorgehensweisen sind dann doch ähnlich.

IT&P: Was konkret wäre Ihre Aufgabe bei einem solchen Projekt? Sind das Beratungsdienstleistungen? Gehen Sie tatsächlich ins Unternehmen und führen das Assessment durch – von A bis Z?

Kruschitz: Aktuell werden wir von größeren, weltweit operierenden Chemieunternehmen angefragt. Diese Unternehmen wollen einen weltweiten IT-Security-Standard einführen und benötigen genau hier Unterstützung. An diesem Punkt übernehmen wir tatsächlich die Assessments. Insbesondere in der pharmazeutischen Industrie unterstützen wir auch Qualifizierungs- und Validierungsaktivitäten. Im Bereich Anlagensicherheit geht es dann auch so weit, dass wir Emergency-Shutdown-Systeme programmieren, die Inbetriebnahme durchführen. Aktuell ist ein Kollege gerade in Norwegen und betreut dort ein sehr großes Emergency-Shutdown-System im laufenden Betrieb – vom Assessment bis zur Unterstützung im laufenden Betrieb.

IT&P: Warum machen Betriebe so etwas nicht intern? Gibt es dort keine Spezialisten oder ist da ein externes, neutrales Bewertungssystem gefragt?

Kruschitz: Es gibt zwei Gründe, warum man zu einem externen Partner geht. Der eine ist: Ich habe eine neutrale Person im Team, dies ist insbesondere bei Assessments wichtig. Diese Person steuert das Projekt und moderiert Risikoanalysen. Risikoanalysen sind immer auch interdisziplinäre Projekte. Da habe ich es üblicherweise mit Vertretern aus der Produktion, der IT-Abteilung und der Automatisierung zu tun; im Prozessumfeld auch mit der Verfahrenstechnik. Vor allem steht diese neutrale Person nicht im Verdacht, der ein oder anderen Partei nahe zu stehen. Zum zweiten ist das Thema IT-Security in der Produktion Neuland. Was die Anlagensicherheit betrifft: Damit beschäftigt man sich seit Jahren sehr intensiv. Auch GMP-Fragestellungen sind mittlerweile etabliert. Bedingt durch den technologischen Fortschritt sowie durch neue Normen, ist dieses Feld für viele Firmen neu zu bestellen. Daher sind diese Firmen dankbar für Partner, die externe Erfahrung mitbringen.

IT&P: Wie weit ist das Bewusstsein für Sicherheit im Umfeld der MES-Systeme gediehen?

Kruschitz: MES-Technologie ist ein Treiber: Dadurch, dass ein MES Anlagenteile miteinander vernetzt, entstehen IT-Security-Risikopotenziale. Dort, wo früher eine Maschine in der Halle stand und isoliert betrieben wurde, ist sie jetzt in den IT-Unternehmensverbund einbezogen. Diese Einbeziehung heißt aber eben auch, dass wechselseitige Bedrohungen entstehen. Durch die MES-Technologie ist IT-Security in der Produktion überhaupt erst zum Thema geworden. Wie ist man dem bis dato entgegen getreten? Ich glaube, die Systemhersteller – zumindest die großen – sind aktuell dabei, ihre Systeme sicher zu gestalten. Das heißt, dass sie während der Entwicklungsarbeit schon darauf achten, dass im späteren Betrieb eine Sicherheitsorganisation maßgeschneidert werden kann. Die momentan im Betrieb befindlichen Systeme weisen in dieser Hinsicht Schwachstellen auf, die der Benutzer durch sein Eingreifen in die Sicherheitsorganisation zu lösen hat. In Zukunft werden diese Systeme von Haus aus robuste Mechanismen zur bequemen Konfiguration mit sich bringen. Der Aufwand, der in vier oder fünf Jahren für Sicherheit in der Produktion zu betreiben sein wird, wird – das werden wir sehen – wesentlich geringer sein.

IT&P: Gibt es Standards oder Normen, an denen man sich aus Betreibersicht halten kann, wenn man ein IT-Security-Asssessment für ein MES durchführen möchte?

Kruschitz: Standards sind ein schwieriges Thema. Die etablierten Standards beziehen sich auf die normale Unternehmens-IT, auf die Office-Welt. Uns – auf der MES- oder Automatisierungsebene – bieten diese Guidelines, jedoch keine Antworten auf die spezifischen Anforderungen. Die Automatisierungswelt ist gerade erst dabei, hier Standards zu schaffen. In Deutschland arbeitet der VDI hieran federführend, international ist es die ISA mit der ISA99, die zumindest aus meiner Sicht einen sehr umfangreichen Ansatz produzieren. Bis ein Standard steht, der zumindest in der Prozessindustrie einsetzbar sein wird, dauert es aber mit Sicherheit noch zwei Jahre.

IT&P: Kann ein Kennzahlensystem helfen, ein Assessment durchzuführen?

Kruschitz: Wir haben aus den existenten Normen wie dem Grundschutzhandbuch die Punkte abgeleitet, die für unsere Arbeit in der Prozessindustrie relevant sind. Das ist der Anapur-Standard – ein Provisorium. Wir erwarten, dass durch die ISA99 ein quantitativer Katalog erbracht werden wird.

IT&P: Innovation und Sicherheit scheinen Gegenpole zu sein. Wie wird sich dieser Widerspruch in den kommenden zehn Jahren entwickeln?

Kruschitz: Wünschenswert wäre, wenn sich die beiden Gegenpole treffen und Sicherheit schon in der Entwicklungsphase ein Parameter wird. Ein MES sollte also nicht nur neue Features, bessere Performance, neue Kommunikationswege wie Wireless oder neue Bedienoberflächen bekommen. Ich habe das starke Gefühl, dass das auch passieren wird und dass Sicherheit schon bei den kommenden Entwicklungsschritten eine große Rolle spielen wird.

IT&P: Industrielle Kommunikation und Sicherheit sind ebenso derzeitige Widersacher. Welche Aspekte kommen hier in Zukunft zum tragen?

Kruschitz: Im Umfeld der Prozessindustrie ist das Thema Wireless aktuell ein großes Diskussionsthema – allerdings einmal weniger aufgrund der Sicherheitsaspekte, sondern vielmehr aufgrund der zwei konkurrierenden Standards, über die Sie im Zuge der vergangenen Namur-Hauptversammlung berichtet haben. Sicherheitsfragen werden erst diskutiert werden, wenn klar ist, wohin der Weg führt. Die Prozessindustrie ist hier ein wenig konservativer als die Fertigungsindustrie. Die Hauptfrage wird die sein: Werden wir in der Lage sein, einen Standard zu etablieren? Dann wird sich auch die Frage nach dem Sicherheitsstandard regeln. Ich bin nicht der Meinung, den Einsatz von Wireless-Technologien grundsätzlich zu verteufeln. Sicherlich kann man die Technologie nicht für alle Aufgabenstellungen einsetzen. Wireless hat, was die Verfügbarkeit betrifft, bestimmte Einschränkungen. In diesem Wissen müssen Applikationen vorgesehen werden, die eben auch ohne permanente Kommunikation auskommen. Der mobilste Teil der Anlage ist der Mensch. Daher wird aus meiner Sicht Wireless dort eine große Rolle spielen, wo Informationen zum Menschen transportiert werden müssen. Dort wird man um Wireless gar nicht herumkommen. *(sph)* ■

www.anapur.de