IT-Sicherheit in der Pharmaindustrie

Abwehrkräfte stärken

Nachdem jüngst immer mehr Cyber-Attacken auf IT-Systeme in der Pharmaindustrie abzielten, verlagert sich der Fokus der Angreifer immer mehr auf Produktionssysteme und Steuerungssysteme. Das IT-Sicherheitsgesetz soll Pharmaproduzenten helfen, sich zu schützen. Doch sind die Systeme der pharmazeutischen Produktion darauf vorbereitet?

TEXT: Holger Mettler und Robert Geiger, M+W Central Europe **BILDER:** M+W Central Europe; iStock, Thiago Santos

Die Digitalisierung schreitet voran und erfasst auch die Maschinenparks der pharmazeutischen Herstellung immer mehr. Industrie 4.0 bietet enorme Chancen für Medizintechnik und Arzneimittelproduktion. Doch gerade in dieser eher konservativen Branche bringt die digitale Vernetzung von Produktionsanlagen große Sicherheitslücken mit sich, wenn die Netzwerke nicht wirkungsvoll gegen Angriffe abgesichert sind.

Dass die Pharmaindustrie noch Nachholbedarf in puncto Cyber-Security hat, beweisen Wannacry und Petya/NotPetya: Von den beiden großen Malware-Attacken waren unter anderem mehrere Krankenhäuser des englischen Gesundheitssystems und der US-amerikanische Pharmakonzern Merck betroffen. Kriminelle hegen im Gesundheitsbereich großes Interesse an digitalen Spionage- und Sabotageakten, geht es doch besonders bei neuen medizinischen Entwicklungen um hohen Wettbewerbsvorteil, Umsätze und somit bares Geld.

Automatisierte Produktion schützen

Um das Gesundheitswesen künftig besser abzusichern, hat die Bundesregierung im Juni 2017 die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) angepasst, die Teile der Pharmaindustrie dem strengen IT-Sicherheitsgesetz unterwirft. Mit der Änderungsverordnung des IT-Sicherheitsgesetzes wurden abschließend die Kriterien für den Sektor Gesundheit bestimmt. Demnach sind medizinische Versorger – neben Krankenhäusern und Laboren gehören dazu auch Pharmaunternehmen – dazu verpflichtet, ihre Systeme nach der Kritis-Verordnung abzusichern.

Der zweite Korb des Gesetzes thematisiert auch die Absicherung pharmazeutischer Produktionsanlagen und die dazugehörige IT. Ein umfassendes Sicherheitskonzept betrifft in der Pharmaindustrie nicht nur die IT-Systeme, sondern auch automatisierte, computerisierte Produktionssysteme. Zur Automation von GMP-konformen Herstellungsprozessen, beispielsweise an Abfüll-, Misch- und Verpackungsanlagen oder bei der Überwachung von Reinräumen, kommen immer häufiger industrielle Steuerungssysteme zum Einsatz. Digital vernetzte Computersysteme unterliegen jedoch denselben Cyber-Sicherheitsrisiken wie die klassische Unternehmens-IT.

Das hat zur Folge, dass frühere Ingenieursaufgaben heute Fälle für die IT-Abteilung sind. Demnach müssen die automatisierten und digitalisierten Anlagen mit Informationssicherheitsmanagementsystemen ausgestattet sein, die komplexe IT-Systeme an einzelnen Produktionsmaschinen und innerhalb des Maschinenparks zuverlässig schützen. Die Anforderungen an die Cyber-Security über den gesamten pharmazeutischen Herstellungsprozess sind durch die Kritis-Verordnung nun klar abgesteckt.

Pharmaproduktion ist jetzt in der Pflicht

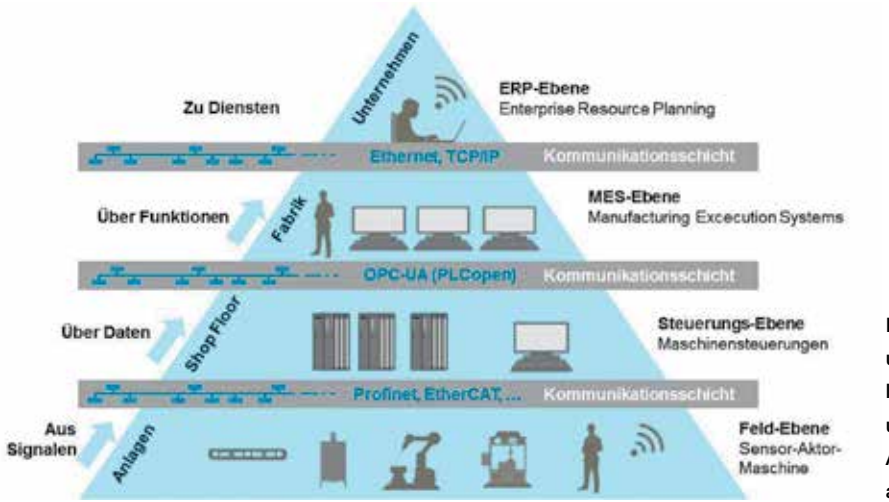
Die Cyber-Absicherung der Produktionsanlagen stellt die Branche jedoch vor eine Herausforderung: „Viele der Anlagen, die in der pharmazeutischen Produktion zum Einsatz kommen, sind dort über 20 Jahre hinweg in Betrieb. Das bedeutet, dass auch häufig veraltete Computertechnik im Einsatz ist“, erklärt Holger Mettler, Leiter Computer System Validation bei M+W Central Europe. „Die neue Generation von Anlagen ist allerdings hoch technologisiert und mit anderen Systemen vernetzt. Auf solche komplexen IT-Systeme ist die pharmazeutische Produktion noch nicht vorbereitet“, so Mettler.

Folglich schaffen sich Unternehmen, die solche Maschinen einsetzen, unter Umständen eine Sicherheitslücke, von der sie bisher noch gar nichts wussten. „Und in der Regel gibt es in der Produktion auch

keinen IT-Spezialisten, der sich um Viren oder Trojaner in Produktionssystemen kümmert. Dadurch ist das Thema brandheiß“, betont Mettler.

Pharmaunternehmen müssen also eine geeignete Lösung finden – und die Zeit läuft: Das erweiterte Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in Bezug auf die Gesundheitsindustrie gibt betroffenen Unternehmen bis spätestens 2019 Zeit, um die Anforderungen zu erfüllen. Deshalb sind die produzierenden Pharmabetriebe nun in der Pflicht, wirksame Informationssicherheitsmanagementsysteme (ISMS) einzuführen.

In erster Linie gilt es hierbei, Standards für die Pharmabranche festzulegen. Das IT-Sicherheitsgesetz besagt, dass die Firmen einen Sicherheitsbeweis für ihren Stand der Technik erbringen müssen. Wie sich dieser gestaltet, wird sich in den nächsten Monaten zeigen. Vertreter und Abgesandte betroffener Firmen werden dazu in Gremien und Arbeitskreisen einen Sicherheitsstandard für die Pharmabranche erarbeiten, an den es sich als Betreiber und Zulieferer einer pharmazeutischen kritischen Infrastruktur zu halten gilt. In der Automobilindustrie beispielsweise müssen sich die beteiligten Unternehmen, Zulieferer und Dienstleister an die für die-



Durch die zunehmende Digitalisierung und die Anbindung von Automationslösungen müssen vernetzte Anlagen und ihre Schnittstellen hinsichtlich der Anforderungen an die Cyber-Security ausreichend abgesichert werden.

sen Sektor festgelegte Regularien halten, um eine sicherheitswirksame Auftragsabwicklung zu garantieren.

„Der allgemeingültige Standard, falls er denn überhaupt kommen wird, wird allerdings voraussichtlich erst in ein, zwei Jahren festgesetzt. Das Gesetz besagt aber, dass jedes Unternehmen bis dahin ein Informationssicherheitsmanagement eingeführt haben muss", weiß Holger Mettler. „Auch andere Branchen, wie die Wasser- oder Elektrizitätswirtschaft, haben vor zwei Jahren die Kritis-Anforderungen unterschätzt. Es war ihnen nicht bewusst, dass hochkomplexe computerisierte Systeme im Einsatz sind, die teilweise ungeschützt darnieder lagen. Daher sind sie hoch gefährdet – ebenso wie die Anlagen der Pharmabranche. Kritis hilft, einen umfassenden Schutz dieser Branchen aufzubauen."

Nicht erst auf den Standard warten

Zwar haben betroffene Kritis-Betreiber nun für die Umsetzung der Sicherheitsrichtlinien nach dem aktuellen Stand der Technik noch ein Jahr Zeit, dennoch ist es ratsam, frühzeitig die Absicherung und Einführung eines Security-Systems in betroffenen vernetzten Produktionsanlagen anzugehen. Ein verlässliches und vertrauenswürdiges Informationssicherheitsmanagement hilft Unternehmen dabei, sich erfolgreich gegen eventuelle Hacker-Angriffe zu wehren und bringt ihnen einen eindeutigen Wettbewerbsvorteil.

Robert Geiger, Berater im Bereich Computer System Validation bei M+W Central Europe, kennt die Notwendigkeit der Anlagenabsicherung: „Die Pharmaindustrie schwimmt bei Industrie 4.0 mit, davor kann sich keiner drücken. Es ist zwingend notwendig, dass sie auch beim Thema Security top aufgestellt ist. Und das ist die Branche derzeit noch nicht. Deshalb wird es höchste Zeit, denn die Angreifer werden immer einfallsreicher und die Auswirkungen einer Attacke können Unternehmen, ihren Kunden und Patienten erheblichen Schaden zufügen. Das gilt es in jeder Hinsicht zu vermeiden."

Bis es einen Kritis-konformen Standard für die Medizintechnik, Arzneimittelproduktion und weitere Unternehmen der pharmazeutischen Industrie gibt, können sich Unternehmen und ihre Zulieferer über den ISO 27001 Standard ein gültiges Informationssicherheitsmanagement einrichten. Eine ISO-27001-Zertifizierung etwa auf der Basis von IT-Grundschutz dokumentiert die Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen. Um diese Zertifizierung zu erhalten, müssen gewisse Anforderungen erfüllt werden. Zudem dauert der Zertifizierungsprozess in der Regel zwischen 12 und 18 Monate. Daher empfiehlt es sich für Pharmaunternehmen, frühzeitig den Rat von branchenerfahrenen Experten einzuholen. Fachleute mit praktischem Know-how bringen die nötige Erfahrung mit und erkennen schnell, welche Bereiche der vernetzten Produktion am gefährdetsten sind und wie diese mit der richtigen Systemarchitektur manipulationssicher gemacht werden können.

Experten frühzeitig ins Boot holen

„M+W möchte Unternehmen möglichst schnell auf den richtigen Weg bringen, damit sie ihre Anlagen ausreichend gegen mögliche Angriffe von außen abschirmen können. Dafür sind Erfahrung, gute Kenntnis der Anlagen und Maschinen sowie umfassendes Computerwissen notwendig, das in den Unternehmen häufig nicht ausreichend vorhanden ist", so Robert Geiger. „Wir unterstützen unsere Kunden in dieser Hinsicht. Unsere Experten begleiten Unternehmen bei der Einführung eines Informationssicherheitsmanagementsystems nach ISO 270001 – von der Definition bis zur Umsetzung der Maßnahmen." ☐

ACHEMA2018 **Halle 9.1, Stand B3**