



Durch die zunehmende Digitalisierung der Pharmaproduktion rückt das Thema Cybersicherheit in den Fokus

Holger Mettler ist Head of Computer System Validation and Cyber Security bei Exyte

Höchste Standards für Datenintegrität und Cybersicherheit

IT-Sicherheit rückt mehr und mehr in den Fokus

In einer digitalen Welt, die sich mehr und mehr vernetzt, muss sich die Pharma- und Biotechbranche verstärkt mit dem Thema Cybersicherheit in der Produktion auseinandersetzen. Sobald eine Produktionsanlage mit Inter- oder Intranet verknüpft wird, übertragen sich die Gefahren für IT- und Cybersicherheit auch auf die Produktion. Was das bedeutet, darüber haben wir mit Holger Mettler, Head of Computer System Validation and Cyber Security bei Exyte, gesprochen.

Herr Mettler, die Pharmaproduktion ist hoch reguliert. Gilt das auch für die IT-Sicherheit oder gibt es hier Defizite?

Mettler: Neben Patientensicherheit und Produktqualität ist die Datenintegrität mittlerweile als wichtiges regulatorisches Thema in den Fokus gerückt. Sie hat sich zunehmend in den digitalisierten Bereich verlagert. Dort ist es in den letzten Jahren zu Manipulationen gekommen, was auch dazu geführt hat, dass Produkte vom Markt genommen wurden. Der Grund waren u. a. auf elektronischem Wege gefälschte Analyse- und Produktionsergebnisse. Inspektoren prüfen deshalb stark auf Datenintegrität, vor allem in der Analytik, weil dort die Gefahr am größten ist. Ähnliches sehen wir inzwischen in der Produktion: Manchmal ist der Zugriff auf die Computeranlagen in der Produktion sehr leicht, weil diese oft nicht geschützt sind. Manche Computer- und Betriebssysteme sind zudem veraltet und können leicht von Viren oder Trojanern infiziert werden.

Sicherlich gibt es aber auch andere Beispiele.

Mettler: Ja, natürlich. In dem Zusammenhang möchte ich gerne auf eines unserer Projekte als positives Beispiel verweisen: Exyte und

die Kantonsapotheke Zürich (KAZ) wurden erst kürzlich mit dem ISPE Facility of the Year Award in der Kategorie Operational Excellence ausgezeichnet. Dieses Projekt zeigt eindrucksvoll, wie die Krankenhausapotheke der Zukunft aussehen sollte und etabliert Standards für die betriebliche Exzellenz, die bislang in solchen patienten-zentrierten Einrichtungen undenkbar waren. Alle relevanten Labor- und Produktionsdaten werden in einem Cloud-basierten, nach ISO 27001 zertifizierten IT-Datencenter gesammelt und zentral gespeichert, um höchste Standards für Datenintegrität und Cybersicherheit zu gewährleisten. Dabei wurde eine vollständig elektronische Dokumentation erstellt, die den Anforderungen von 21 CFR part 11 und Alcoa entspricht.

Muss ein IT-Sicherheitssystem ganzheitlich sein oder kann man es sich auf Teile einer Anlage beschränken?

Mettler: Bei IT- und Cybersicherheit gibt es unterschiedliche Herangehensweisen, die in Kombination einem ganzheitlichen Ansatz nahekommen. Technisch, indem man zu Maßnahmen wie Virenschutz oder Firewall greift. Organisatorisch, indem man ein Identi-



Bild: Ivan Traimik – Fotolia.com

Pharmaunternehmen sind zwar noch nicht dazu gezwungen, ein ISO-27001-Zertifikat zu erbringen, aber sie müssen nachweisen, dass sie ein analoges Modell zum Informationssicherheitsmanagement aufgebaut haben

tätsmanagement einrichtet, das den Zugriff auf bestimmte Anlagen stark beschränkt, was Good Manufacturing Practice (GMP) immer schon erfordert. Prozedural, durch ein ganzheitliches Informationssicherheitsmanagement, wofür es bestimmte Normen und Standards gibt. Verbreitet ist ISO 27001 oder speziell für Deutschland der Grundschutz vom BSI (Bundesamt für Sicherheit in der Informationstechnik), der den Sicherheitszustand einer Infrastruktur bewertet und daraus Maßnahmen entwickelt. Das ist aufwendig und kann zertifiziert werden.

Wie lassen sich bestehende Pharmaanlagen IT-sicher(er) machen?

Mettler: Bei einer automatisierten Pharmaproduktion muss die Herstellung auf vielen Ebenen und Punkten vor Cyberattacken geschützt werden. Produktionsparameter sind aus GMP-Sicht und aus Sicht der IT-Sicherheit kritisch. Um sie herum muss man Schutz-

„Bei einer automatisierten Produktion in der Pharmaindustrie muss die Herstellung auf vielen Ebenen und Punkten vor Cyberattacken geschützt werden.“

schalen bauen. Bei klassischen Anlagen, die noch nicht am Netz sind, setzt man auf Vertrauen, was aber gefährlich ist, weil es Hierarchien braucht, die den Datenzugriff regeln. Kritische Daten dürfen nur von geschultem Personal und unter Einschaltung der Qualitätssicherung und -kontrolle verändert werden.

Was muss bei neuen Anlagen bedacht werden?

Mettler: Die Industrie hat für die Sicherheit von Industrial Control Systems (ICS) einen neuen Standard (ICE 62443) entwickelt. Da geht es unter anderem um Netzwerksicherheit und verschlüsselte Daten. Darüber hinaus gibt es das ISO 27001-Konzept, das auch für das Informationssicherheitsmanagement gilt und sich auch auf die Produktion übertragen lässt. Allerdings greifen Maßnahmen wie Virenschutz im Produktionssystem häufig nicht, weil Maschinen lange laufen müssen und ein im Hintergrund laufender Virenschutz dazu führen könnte, dass die Produktion eventuell stillsteht.

Exyte ist eines der weltweit führenden Unternehmen im Bereich der Planung, Entwicklung und Konstruktion von High-Tech-Fabriken und Anlagen und hat eine besondere Expertise für kontrollierte und regulierte Fertigungsumgebungen. Cyber Security von komplexen Anlagen und vernetzten Systemen ist dabei eine Kernkompetenz des Unternehmens. Das Angebotspektrum erstreckt sich über den gesamten Lebenszyklus von Automatisierungs- und Produktionsdatensystemen – von der IT-Security-Beratung bei der Betreiberanforderung bis hin zur Umsetzung von Informationssicherheitsmanagementsystemen für IT und Produktion. Exyte begleitet mit seinen Kooperationspartnern aus Wissenschaft und Technik auch den Zertifizierungsprozess (z. B. nach ISO 27001) und kooperiert hier u. a. mit dem TÜV Rheinland und dem TÜV Süd. So verbindet das Unternehmen Kompetenz und Erfahrung aus Anlagenbau und Prozesstechnik mit GMP-konformer Automation und IT.

Gibt es eine amtliche Überwachung für IT-Sicherheitsstandards in der Pharmaproduktion?

Mettler: 2017 hat der Gesetzgeber auch die Arzneimittelversorgung zur kritischen Infrastruktur erklärt, womit nun auch Teile der Pharmaindustrie – in Deutschland sind das ca. 120 bis 150 Unternehmen – zur kritischen Infrastruktur zählen. Das Bundessicherheitsgesetz (BSIG) bestimmt, dass Betreiber kritischer Infrastrukturen ihre IT-Systeme, IT-Komponenten und IT-Prozesse durch angemessene Vorkehrungen nach dem Stand der Technik gegen Störungen der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität schützen müssen. Zudem müssen sie dem BSI eine Kontaktstelle benennen und erhebliche Störungen ihrer IT melden. Pharmahersteller mit kritischer Infrastruktur erarbeiten zurzeit einen branchenspezifischen Standard, der in Zusammenarbeit mit dem BSI erstellt wird.

Was bedeutet das letztendlich für die Pharmaunternehmen?

Mettler: Die Datenintegrität ist bereits in den GMP-Regularien verankert und deshalb an sich nichts Neues. Neu ist hingegen, dass der Gesetzgeber verlangt, dass die Firmen tätig werden und ihre Bemühungen zur IT-Sicherheit nachweisen müssen. Das ist ein zertifizierter Prozess. Zwar sind sie noch nicht dazu gezwungen, ein ISO-27001-Zertifikat zu erbringen, aber sie müssen nachweisen, dass sie ein analoges Modell zum Informationssicherheitsmanagement aufgebaut haben.

www.prozesstechnik-online.de

Suchwort: phpro0319exyte



DAS INTERVIEW FÜHRTE FÜR SIE MARIA WIDRA

Manager External Communication & Public Relations, Exyte