Seiten-Adresse:
https://www.gesundheitsindustrie-bw.de/fachbeitrag/aktuell/cybersecurity-ist-fuer-die-pharma-produktion-ein-wichtiges-thema

Experteninterview

Cybersecurity ist für die Pharma-Produktion ein wichtiges Thema

In einer immer mehr vernetzten Welt muss sich die Pharma- und Biotech-Branche mit der Cybersecurity in der Produktion beschäftigen. Was das bedeutet, darüber haben wir mit Holger Mettler gesprochen. Der 54-Jährige verantwortet den Bereich Computersystemvalidierung und Cybersecurity bei Exyte (früher M + W), einem global tätigen Unternehmen für Planung, Engineering und Errichtung komplexer Produktionsanlagen und Gebäude für die Life-Science-Industrie. Weltweit sind für die Exyte Group über 5.000 Mitarbeiter tätig. Mettler hat Kommunikationstechnik, Bionik und Informatik studiert.

Holger Mettler, Fachmann für Cybersecurity.

Ist die wachsende Vernetzung von Maschinen und Menschen auch in der Pharma-Industrie angekommen?

Ja, sie ist dort angekommen. Viele Firmen, vor allem solche, die in ihren Anlagenpark neu investieren müssen, wissen, dass ihre Zulieferer stark auf digitalisierte und informationstechnisch ausgerüstete Systeme setzen. Es wird zunehmend das Konzept der papierlosen Produktion favorisiert. Leider setzen manche Hersteller noch stark auf Papier. In der Produktion ist das meiner Meinung nach noch nicht richtig angekommen.

Erhöht die IT-Vernetzung in Pharma-Anlagen die Anforderungen an die Cybersecurity?

Auf jeden Fall. In der Produktion sprechen wir von hochkritischen Anlagen. Dort muss zunächst die funktionale Sicherheit geschützt sein, was klassische Mechatronik leistet. IT-und Cybersicherheit beziehen sich nicht nur auf eine einzelne Anlage, sondern auf einen Cyber-Raum, wo Anlagen aus Verpackung, Abfüllung oder Medienversorgung miteinander vernetzt sind und Daten austauschen. Daten im Pharmasektor sind mittlerweile in verteilten Data Centern

aufgeladen, nicht länger standortgebunden, befinden sich in der Cloud. Sobald Inter- oder Intranet mit der Produktion verknüpft wird, überträgt man diese Gefahren für IT- und Cybersicherheit auf die Produktion.

Die Pharma-Produktion ist hoch reguliert. Gilt das auch für die IT-Sicherheit oder gibt es Defizite?

Neben Patientensicherheit und Produktqualität ist die Datenintegrität als wichtiges regulatorisches Thema in den Fokus gerückt. Sie hat sich zunehmend in den digitalisierten Bereich verlagert. Dort ist in den letzten Jahren manipuliert worden, was auch dazu geführt hat, dass Produkte vom Markt genommen wurden. Da wurden Analyse- und Produktionsergebnisse auf elektronischem Wege gefälscht. 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 sie oft nicht geschützt sind. Manche Computersysteme sind veraltet und können leicht von Viren oder Trojanern infiziert werden.

Ist die Pharma-Industrie Zielscheibe von Cyber-Angriffen?

Ja, sie wird seit längerem aus dem Internet angegriffen. Gelingt es, an Daten aus FuE oder Produktion zu kommen, werden Pharmafirmen erpressbar. Der WannaCry-Virus 2017 befiel überraschenderweise bei betroffenen Pharmafirmen nicht nur Office-Rechner, sondern auch Produktionsrechner. Bei einigen Firmen soll die Produktion deshalb einige Tage geruht haben.

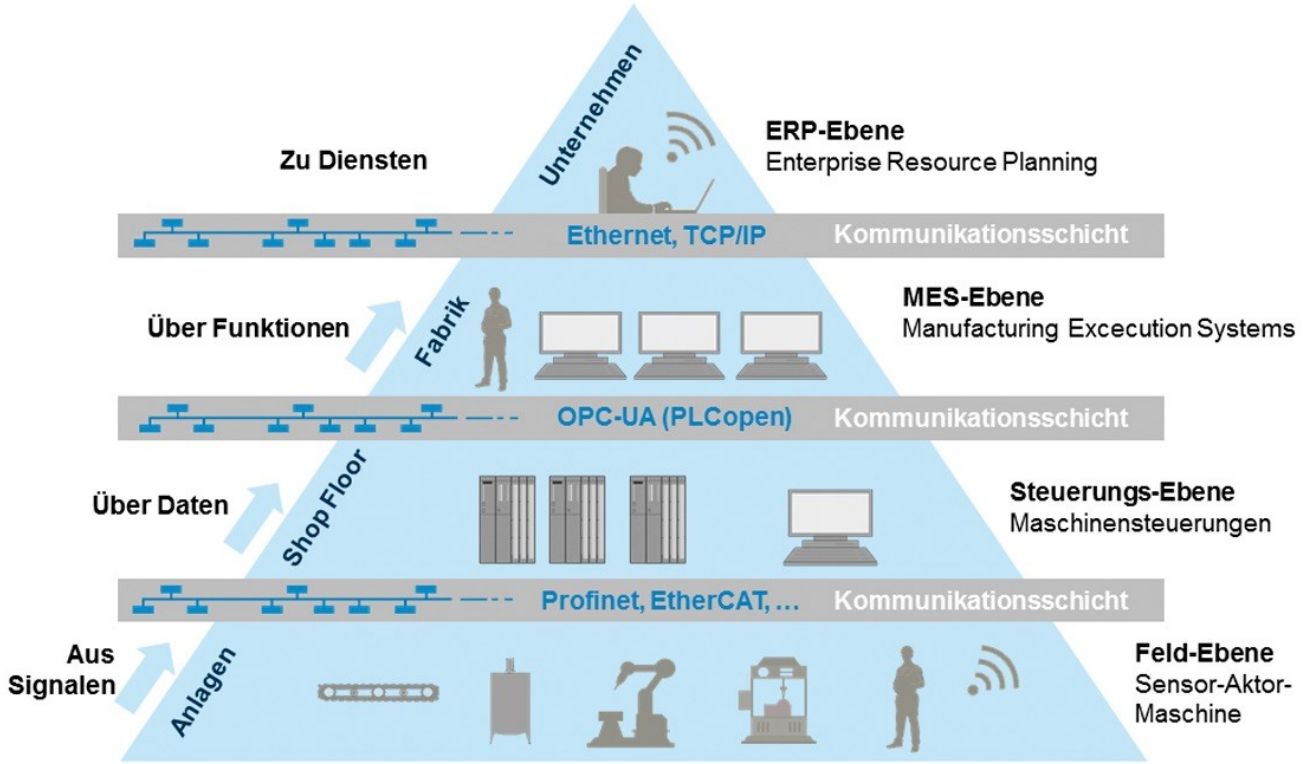
Dazu muss man wissen, dass die automatisierte GMP-Produktion von ‚Industrial Control Systems' (ICS) gesteuert wird. Während alte Systeme oft noch autonom sind, bestehen neue zunehmend aus automatisierten, untereinander kommunizierenden kleinen Systemen.

Problematisch sind auch Fernwartungszugänge, die Zulieferer Pharmafirmen anbieten. Damit haben diese direkten Zugang in ein Netzwerk, das sich zwar gut absichern lässt. Allerdings kennt man die Person auf der anderen Seite nicht. Zulieferer verlassen sich bei Cloud-Lösungen auf IT-Dienstleister, die Rechenzentren betreiben. Unter GMP-Gesichtspunkten ist das fatal, weil diese fordert, dass jede kritische Aktivität nachvollziehbar ist. Schauen Externe auf das System, gibt man die Daten frei. Das Stuxnet-Virus hat gezeigt, dass sich über einen Drucker ein industrielles Kontrollsystem zerstören lässt.

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

In IT- und Cybersicherheit gibt es unterschiedliche Ansätze, die in Kombination einem ganzheitlichen Ansatz nahekommen. Technisch, indem man zu Maßnahmen wie Virenschutz oder Firewall greift. Organisatorisch, indem man ein Identitätsmanagement einrichtet, das den Zugriff auf bestimmte Anlagen stark beschränkt, was GMP immer schon erfordert. Prozedural, durch ein ganzheitliches Informationssicherheitsmanagement, wofür es bestimmte Normen und Standards gibt. Verbreitet ist ISO 27001 oder speziell für Deutschland vom BSI (Bundesamt für Sicherheit in der Informationstechnik, d. Red.) der BSI-Grundschutz, der den Sicherheitszustand einer Infrastruktur bewertet und daraus Maßnahmen entwickelt. Das ist aufwendig und kann zertifiziert werden.

Wie lassen sich bestehende Pharma-Anlagen IT-sicher(er) machen? Was muss bei neuen Anlagen bedacht werden?



Das Schaubild einer automatisierten Pharmaproduktion zeigt anschaulich, auf wie vielen Ebenen und Punkten die Herstellung sich vor Cyber-Attacken schützen muss.

Produktionsparameter sind aus GMP-Sicht und aus Sicht der IT-Sicherheit kritisch. Um sie herum muss man Schutzschalen 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. Ähnlich sieht es im IT-Bereich aus, wo man stets überlegen muss, an welcher Stufe welche Sicherheitsnorm oder welcher Sicherheitsstandard geschaffen werden soll.

Die Industrie hat für die Sicherheit von ICS einen neuen Standard (ICE 62443) entwickelt. Da geht es unter anderem um Netzwerksicherheit und verschlüsselte Daten. Das andere ist das ISO 27001-Konzept für das Informationssicherheitsmanagement. Es lässt sich auch auf die Produktion übertragen. Leider ist das in der Industrie noch nicht richtig umgesetzt.

Wichtig ist zu erkennen, dass technische Maßnahmen wie Virenschutz im Produktionssystem nicht funktionieren, weil Maschinen lange laufen müssen und ein im Hintergrund laufender Virenschutz dazu führen könnte, dass die Produktion eventuell still steht. Hier muss man den Zugriff auf dieses System so weit wie möglich beschränken.

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

2017 hat der Gesetzgeber auch die Arzneimittelversorgung zur kritischen Infrastruktur erklärt und damit Teile der Pharmaindustrie – in Deutschland sind das ca. 120-150 Firmen – hineingenommen. Das Bundessicherheitsgesetz (BSIG) bestimmt, dass Betreiber kritischer Infrastrukturen ihre kritischen 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 auch einen branchenspezifischen Standard, der in Zusammenarbeit mit dem BSI erstellt wird.

Eigentlich ist die Datenintegrität in den GMP-Regularien verankert und deshalb nichts Neues. Neu ist, dass der Gesetzgeber verlangt, dass die Firmen tätig werden müssen 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.

Der Leidensdruck der vom Gesetzgeber ins Visier genommenen Pharma-Unternehmen steigt also?

Der Leidensdruck wird auch durch die wachsende Zahl der Inspektionen, bei denen die Datenintegrität stets eine große Rolle spielt, zunehmen. So sind auch deutsche Unternehmen von der FDA mit einem ‚Warning Letter' wegen fehlender Datenintegrität betroffen gewesen. Daten- und Informationssicherheit sind im Prinzip nahezu das Gleiche. Datenintegrität bedeutet ja, dass man an bestimmten Stellen nachweisen kann, dass die Daten nicht manipuliert worden sind. Zukünftiges Ziel muss es sein, die IT-Sicherheit und die GMP-Anforderungen auch unter Kostengesichtspunkten zusammenzuführen.

Literatur:

VO zur Änderung der BSI-Kritisverordnung, 21. Juni 2017, ergänzt um die KRITIS Gesundheit:
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1903.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1903.pdf%27%5D__1543301401959

Initiative zur kompletten Vernetzung innerhalb der Pharma-Produktion:
https://ispe.org/initiatives/pharma-4.0#