Digital? Aber sicher!

Mit der richtigen Cybersecurity-Strategie Produktionsprozesse sichern

Die Life-Sciences-Branche denkt bei der digitalen Transformation vor allem an die Optimierung bestehender Prozesse. Die Kehrseite davon: Mit dem wachsenden Datenstrom haben auch die potenziellen Sicherheitsrisiken zugenommen. Rino Woyczyk, Partner und Head of Life Sciences des auf Bau und Immobilien spezialisierten Beratungsunternehmens Drees & Sommer, erklärt im Interview, worauf es bei der richtigen Cybersecurity-Strategie ankommt.

Herr Woyczyk, Digitalisierung in der Produktion ist für die meisten Chemie- und Pharmaunternehmen nichts Neues. Warum hat das Thema für Sie gerade jetzt so große Relevanz?

Rino Woyczyk: Cyberattacken sind Teil der modernen Kriegsführung – das sehen wir deutlich am Beispiel des Ukraine-Kriegs. Zahlreiche Unternehmen werden aktuell durch Cyberkriminelle angegriffen. Sogar das Bundeskriminalamt wurde zum Ziel. Der Krieg schwappt im Cyberraum damit auch auf deutsche Unternehmen über. Und die Life-Sciences-Industrie ist als wichtiges Rückgrat der deutschen Wirtschaft ein potenziell attraktives Angriffsziel für Hacker. Wenn Produktionsprozesse gestört oder gar komplett lahmgelegt werden, gerät die Versorgungssicherheit mit Wirkstoffen und Medikamenten ins Wanken. Das muss unter allen Umständen verhindert werden.

Das ist einfacher gesagt als getan.

R. Woyczyk: Nicht unbedingt. Es geht vor allem darum, die eigenen Schwachpunkte zu kennen und zu eliminieren. In den vergangenen Monaten haben wir bei unterschiedlichen Kunden in der Branche einen sogenannten Digital Ready Check durchgeführt. Wir prüfen dabei Produktionsgebäude und sonstige Liegenschaften wie Verwaltungsgebäude, Logistik und Versorgungsgebäude auf Herz und Nieren, was die IT-Infrastrukturen, Konnektivität, Cybersecurity und die technische Infrastruktur angeht. Dabei finden wir immer wieder die gleichen Schwachpunkte.

Welche Schwachstellen sind das?

R. Woyczyk: Nehmen wir beispielsweise die technische Gebäudeausrüstung und die Gebäudeautomation. Wer sich hier Zugriff verschafft, kann die Luftmengen, Temperatur- oder Feuchtewerte ganz einfach verändern – mit verheerenden Folgen für die GMP- und FDA-Regularien. Und es ist nicht nur die Software, die Risiken birgt. Unter vielen Gebäuden befindet sich eine zugängliche Tiefgarage mit einer Be- und Entlüftungsanlage. Hierüber können sich Dritte relativ einfach ins Gesamtanlagensystem einhacken und Manipulationen für andere Bereiche vornehmen. Dazu kommt, dass Gebäudeautomationsregelungssysteme mit ihren Schaltschränken oft in Technikzentralen ohne jegliche Zugangssicherung verbaut. Segmentierte IT-Netze fehlen, und sichere Passwörter sind in der Regel ebenfalls nur unzureichend vergeben. Die Zugangsports zu den Gebäudeautomationssystemen sind meist offen für externe Zugänge, ebenso wie aktive Netzwerkkomponenten. Das Facility Management greift normalerweise remote über einen VPN-Kanal mit angeschlossener FRITZ!Box zu. Die unternehmenseigene IT kennt diese Zugänge oftmals nicht. Die Produktionsprozesse sind damit leicht manipulierbar.

> *Die Life-Sciences-Industrie ist als wichtiges Rückgrat der deutschen Wirtschaft ein potenziell attraktives Angriffsziel für Hacker.*
>
> Rino Woyczyk, Partner und Head of Life Sciences, Drees & Sommer

Wie können sich Unternehmen davor schützen?

R. Woyczyk: Grundsätzlich gilt: Datenschutz muss von Anfang an Bestandteil jeder Digitalisierungsstrategie sein. Data protection by default lautet hier der Grundsatz, an dem alle Digitalisierungsbausteine ausgerichtet werden sollten. Wir haben uns bei Drees & Sommer hierfür mit dem IT-Dienstleister ComConsult einen erfahrenen Kooperationspartner ins Boot geholt, mit dem wir gemeinsam eine Cybersecurity-Strategie für Gebäude und Produktion entwickelt haben. Wie wichtig das ist, hat zuletzt das Bundesamt für Sicherheit in der Informationstechnik unterstrichen, das unseren neuen Cybersecurity-Standard seit Februar 2022 als verbindlich ansieht.

Das gilt aber nur für Gebäude und Anlagen, die neu gebaut werden. Wie können Unternehmen Cybersecurity im Bestand bewerten?

R. Woyczyk: Zunächst definieren wir verschiedene potenzielle Bedrohungsszenarien. Nehmen wir beispielsweise Hacker-Angriffe: Um Systeme bestmöglich zu wappnen, testen wir alle Hard- und Software-Applikationen in unserem hauseigenen Testcenter in Aachen in sogenannten Penetration-Tests. Um Sicherheitslücken zu entdecken, konfrontieren wir alle Systembestandteile und Anwendungen mit Mitteln und Methoden, die Hacker anwenden würden, um unautorisiert in das System einzudringen. So können wir feststellen, wie empfindlich ein System ist und daraus Schutzmaßnahmen ableiten. Neben Firewalls, Antivirus-Software und regelmäßigen Updates empfiehlt sich außerdem die Unterteilung des IT-Systems in Netzwerksegmente mit klaren Zugriffsrechten.

Welche weiteren Punkte würden Sie Unternehmen empfehlen?

R. Woyczyk: Für Datendiebstahl, Industriespionage oder digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen können auch die eigenen Mitarbeitenden verantwortlich sein. Auch davor müssen sich Unternehmen bestmöglich schützen. Das fängt schon bei der Benennung eines Datenschutzverantwortlichen an und zieht sich über die Systemkonfiguration von Anlagen bis hin zur Gebäudeautomation. Gleichzeitig ist es wichtig, sich nicht von proprietären Systemen abhängig zu machen. Wer künftig erfolgreich sein will, muss in Systemen und Plattformen denken – das gilt auch für Gebäudeautomation. Als Betriebssystem der Immobilie muss die Gebäudeautomation eine grenzenlose Einbindung sämtlicher Gewerke ermöglichen – und das über die Errichtung hinaus. Zu diesem Zweck muss eine Strategie erarbeitet werden, die eine einfache, effiziente und nachhaltige Einbindung von in und um das Gebäude befindlichen „Dingen" über Protokolle und Bussysteme erlaubt.

■ www.dreso.com

Standardisierte nachrichtenbasierte Kommunikation zwischen MES und Shopfloor

Körber lanciert „PAS-X MSI Plug & Produce"-Programm

Die Kommunikation zwischen dem Equipment auf dem Shopfloor und einem MES (Manufacturing Execution System) kann eine große Herausforderung darstellen, wenn die IT-Systeme über keine gemeinsame Schnittstelle verfügen. Körber, ein Anbieter von MES-Software, hat jetzt ein neues Partnerschaftsprogramm für Anbieter von Maschinen, Equipment und Systemen angekündigt. Mit zwei verschiedenen „PAS-X MSI Plug & Produce"-Partnerschaftszertifikaten können Anbieter nun unter Beweis stellen, dass sie die MSI-Technologie (Message-based Shopfloor Integration) implementieren können.

Werum PAS-X MSI Plug & Produce – eine Erweiterung der PAS-X MES Suite – ermöglicht eine standardisierte, nachrichtenbasierte Kommunikation zwischen dem MES und dem Equipment oder den Maschinen auf dem Shopfloor. Unter Berücksichtigung der branchenüblichen Best Practices lassen sich mit dieser Technologie Maschinen und Automatisierungssysteme schnell und einfach in die pharmazeutische Produktionsumgebung integrieren. Der manuelle Konfigurationsaufwand kann erheblich verringert werden, sodass die Arbeitslast um bis zu 75 % reduziert wird. PAS-X MSI Plug & Produce von Körber wird in der Branche zunehmend als Standard angesehen und implementiert auch das Concept Paper der Plug & Produce Working Group der International Society of Pharmaceutical Engineers (ISPE). Im Geschäftsfeld Pharma bietet das Lüneburger Unternehmen entlang der gesamten Pharmawertschöpfungskette integrierte Softwarelösungen an, die Arzneimittelhersteller bei der Digitalisierung ihrer Pharma-, Biotech- und Zell- & Genfabriken unterstützen.

Mit dem „PAS-X MSI Plug & Produce"-Partnerschaftszertifikat können Anbieter von Equipment, Maschinen oder Systemen nun weltweit Körber Ecosystem Partners werden. „Wir glauben, dass wir zusammen mit unseren Partnern den entscheidenden Unterschied für unsere gemeinsamen Kunden in der Pharma-, Biotech- oder Cell-&-Gene-Branche machen können", erklärt Lars Hornung, Senior Principal Alliances & Technology Partners Software, Körber-Geschäftsfeld Pharma. (mr) ■