Gut geplant, vernetzt und digitalisiert

Robuste und zuverlässige Verpackungslinien für die Petrochemie

Maschinen in petrochemischen Betrieben müssen außerordentlich zuverlässig und robust sein. Denn kommt es zu Ausfällen, können auf den Betreiber Kosten in Millionenhöhe zukommen. Die Beumer Group liefert von der Absackung bis zur Verpackung komplette Verpackungslinien inklusive Service. Der Anwender profitiert von der modularen Bauweise der Maschinen und weiteren Vorteilen durch die zunehmende Vernetzung und Digitalisierung.

Rafael Imberg, Beumer Group

© BEUMER Group GmbH & Co. KG

Am Ende der Prozesskette ist die Verpackungslinie. Steht diese still, weil eine Maschine defekt ist, müssen oft auch andere Anlagen abgeschaltet werden, bspw. die Extruder. Jede Stunde, in der die Produktion stillsteht, kann ein Unternehmen mehrere 100.000 EUR kosten. Dazu kommen Kosten, um das Problem zu beseitigen – etwa für Betriebsmittel, Ersatzteile und Instandhaltung. Nicht zu unterschätzen sind entgangene Geschäftsgelegenheiten und ein geschädigtes Kundenvertrauen. In der Petrochemie wird eine robuste und ausfallsichere Arbeitsweise der Maschinen immer wichtiger, deshalb hat die Beumer Group das Design ihrer Verpackungsanlagen überarbeitet und sie modular aufgebaut.

Der Beumer Fillpac FFS z.B. formt Säcke aus einer vorgefertigten PE-Schlauchfolie und füllt diese zuverlässig und schonend ab. Anschließend werden sie automatisch verschweißt. Bis zu 2.800 Säcke pro Stunde kann die Maschine auf diese Weise handhaben. Nach dem Verschließen werden die Säcke für den Transport sicher und zuverlässig auf einer Palette gestapelt, wofür sich der Beumer Paletpac besonders eignet. Auch dieses System lässt sich individuell an die unterschiedlichen Anforderungen der chemischen Industrie anpassen. Die Anlage erreicht einen Durchsatz von bis zu 3.200 Säcken pro Stunde. Für die Endverpackung hat der Systemanbieter seine Hochleistungsverpackungsanlage Stretch Hood im Programm. Die Stretchfolie passt sich an jeden Stapel an. Sie ist sehr dehnbar und fixiert das Material sowohl durch die horizontalen als auch die vertikalen Rückstellkräfte auf der Palette. Dieses Verfahren bietet so eine hohe Ladungsstabilität.

Modular und intelligent

Alle Baureihen haben die Beumer-Spezialisten nicht nur robust gestaltet, mit der neuen modularen Bauweise sind in den Anlagen auch gleiche oder ähnliche Komponenten und Module verbaut. Das reduziert die Anzahl der Ersatzteile, beschleunigt deren Lieferzeiten und erleichtert dem kundenseitigen Personal die Wartung. Durch das gleiche Look and Feel kann der Mitarbeitende ganz leicht einen Paletpac bedienen, obwohl er bspw. bisher nur mit der Handhabung des Beumer Stretch Hood vertraut war. Das Personal lernt so auch die verschiedenen Maschinen schneller kennen. Die modulare Bauweise schafft noch weitere Vorteile: Fordert der Anwender mehr Leistung, kann diese bei den Maschinen nachträglich relativ einfach gesteigert werden. Ob die Anlage nun nachgerüstet oder ein Schaden behoben werden muss – die Modularität sorgt für einen deutlichen Zeitvorteil.

Auf Wunsch lassen sich auch alle Maschinen und Komponenten mit einer übergeordneten Steuerung – der BG Software Suite – vernetzen. Mit der Visualisierung BG Fusion steht dem Bediener zudem eine webfähige Benutzeroberfläche für Konfiguration, Monitoring und Reporting zur Verfügung. Damit lassen sich alle Informationen, die der Systemanbieter mittels Data Analytics in der Maschine sammelt, transparent darstellen. Maschinendaten, Störmeldungen sowie Hinweise zum Betrieb und zur Wartung werden so aufbereitet, dass der Anwender sie einfach nutzen kann – z.B. für eine vorausschauende Wartung.

©vegefox.com - stock.adobe.com

Wissen, wann die Maschine ausfällt

Denn die Frage lautet: Wie lässt sich die Wartung so planen, dass wir einen plötzlichen Stillstand ausschließen können? Der Kunde möchte z.B. einmal im Monat eine Wartungsschicht. Das heißt, er setzt die Maschinen bewusst still, will aber sichergehen, dass diese danach störungsfrei arbeiten. Bei einem ungeplanten Ausfall hat er nicht immer das erforderliche Werkzeug oder Personal parat, um die Anlage wieder instand zu setzen.

Mit der Datenanalyse lässt sich auch die Einsatzdauer der Komponenten verlängern. Die Kunden wollen wissen, nach wie vielen Betriebsstunden eine bestimmte Komponente, etwa ein Motor, ausgetauscht werden muss. Das lässt sich in der Regel nicht pauschal vorhersagen, weil das immer von den Umgebungsbedingungen abhängt. Wie ist die Maschine eingestellt, wie ist sie gewartet? Besteht die Möglichkeit, etwa Motoren, Sensoren und Zylinder im Betrieb zu überwachen und Schwachstellen elektronisch festzustellen, lässt sich der Austausch auf den optimalen Zeitpunkt festlegen. Ein Beispiel: Wird der Motor ungewöhnlich warm, können die Service-Techniker daraus auf seinen Zustand schließen. Mit dieser Information kann ein plötzlicher Ausfall vermieden werden, denn die Software gibt rechtzeitig Alarm.

Vernetzt vom Silo bis zum Lager

Der Lieferumfang des Systemanbieters Beumer beginnt beim Kunden unterhalb des Silos. Das Produkt fällt in den Sack, dieser wird palettiert und der gesamte Stapel mit einer Stretchfolienhaube überzogen. Über die Beumer Software lässt sich zudem das Warehouse-Management-System (WMS) anbinden. Dieses kann für die Einlagerung etwa über Barcode, RFID oder QR-Code die Waren eindeutig zuordnen. Mit Lesegeräten ausgestatte Gabelstapler „wissen“, wohin sie die Paletten transportieren müssen und geben die Informationen über die Einlagerung zurück ans System. Mit der Software lässt sich das Gesamtsystem vom Silo bis zum Lager vernetzen. Ziel ist es, Schnittstellen zu minimieren und dem Kunden alles aus einer Hand bieten zu können.

Unter dem Stichwort Smart Factory will der Systemanbieter seinen Kunden in Sachen Bedienung und Wartung so viele Aufgaben wie möglich abnehmen. Denn je nach Einsatzort sind auch immer weniger Einsatzkräfte verfügbar.

Service über “voice and picture”

Doch was, wenn trotzdem eine Störung eintritt oder die Maschine komplett ausfällt? Um Betreiber zu unterstützen und längere Ausfallzeiten zu verhindern, schickt Beumer seine weltweit lokalisierten Techniker zum Kunden. Dazu bietet der Customer Support eine 24/7-Hotline. Häufig ist es jedoch nicht möglich, ein komplexes Problem am Telefon schnell und eindeutig zu beschreiben. Für solche Fälle wurde das zukunftsweisende Produkt Beumer Smart Glasses entwickelt. Damit blicken die Servicemitarbeiter virtuell dem kundenseitigen Techniker über die Schulter und gehen gemeinsam mit ihm über Bild und Ton auf Fehlersuche, um diesen zu beheben. Mit den Smart Glasses kann der Kunde schnell ein Bild zum Experten des Systemanbieters schicken, der wiederum auch ein Bild zurücksenden kann. Diese digitale Lösung reduziert zeitaufwändige Anreisen und hohe Zusatzkosten. Next Level of Remote Diagnostic – was früher das Telefon war, ist heute „voice and picture“.

Doch Lösungen werden nicht nur für Greenfield-, sondern auch für Brownfield-Projekte entwickelt. Das ist wichtig, da der Systemanbieter weltweit zahlreiche bereits installierte Anlagen betreut. Viele Kunden entscheiden sich nach Jahren oft für einen Retrofit. Meist ist dies auch unumgänglich aufgrund der Ersatzteilsituation oder Prozessänderungen. Dabei tauschen die Beumer Techniker nicht nur Komponenten, sondern erhöhen über die Software auch die Leistung.

Rafael Imberg, Head of Sales Petrochemie, Beumer Group, Beckum

■ www.beumergroup.de

Cyberbedrohung in der Operational Technology

Schutz vor Angriffen auf Prozessanlagen muss intensiviert werden

Die Cybergefahr für industrielle Systeme steigt seit Jahren. Hacker haben es häufig auf Unternehmensgeheimnisse oder Lösegelder abgesehen. Beim Thema OT-Security muss zügig aufgeholt werden, was lange vernachlässigt wurde.

Im vergangenen Jahr hat die Anzahl der Cyberstraftaten in der Bundesrepublik Deutschland einen neuen Höchststand erreicht. 146.363 Delikte zählte das Bundeskriminalamt (BKA) 2021. Diese Bedrohung macht auch vor der Chemie- und Pharmaindustrie nicht Halt: Schon 2019 enthüllten Datenjournalisten von Norddeutschem Rundfunk (NDR) und Bayerischem Rundfunk (BR), dass eine professionelle Hackergruppe über Jahre hinweg große deutsche Chemie- und Pharmakonzerne ausspioniert hatte. Dazu gehörten Bayer, BASF, Covestro und Henkel. Systeme an der Schnittstelle vom Intranet zum Internet sowie Autorisierungssysteme waren mit Schadsoftware infiziert. Auch Unternehmen im Ausland waren betroffen, darunter der Schweizer Pharmakonzern Roche, der französische Klebstoffhersteller Bostik oder der japanische Chemieriese Shin-Etsu. Der verantwortlichen Gruppe „Winnti“ wird eine Nähe zum chinesischen Staat zugeschrieben.

Sicherheitslage bleibt angespannt

Eine vom Gesamtverband der Versicherer (GDV) in Auftrag gegebene repräsentative Forsa-Umfrage aus dem Jahr 2020 zeigt, wie brisant die Gefahrenlage zu diesem Zeitpunkt bereits war. Dafür wurden die jeweiligen Verantwortlichen für IT-Security in 100 kleinen und mittleren deutschen Chemieunternehmen befragt. 30 % der Befragten gaben an, dass ihr Unternehmen schon einmal Opfer eines Cyberangriffs geworden ist. Während einer Cybersicherheitsanalyse unter 510 mittelständischen Chemieunternehmen wurden zudem bei 41 % der Unternehmen Daten im Darknet gefunden. Darunter waren über 10.000 E-Mail-/Passwort-Kombinationen von Mitarbeitern. Die Situation hat sich mit Beginn des russischen Angriffskrieges in der Ukraine weiter verschärft.

Bewusstsein für OT-Security wächst

Zusätzlich zu den reinen IT-Infrastrukturen sind von der Cybergefahr zunehmend auch industrielle Anlagen betroffen, also Operational Technology (OT). Das verantwortliche OT-Personal war jahrelang allein dafür zuständig, dass Maschinen und Produktionsanlagen zuverlässig laufen. Weil die Systeme komplett abgekoppelt von der IT funktionierten, reichte dies auch aus. OT-Security war deshalb schlichtweg kein Thema. Einhergehend mit Entwicklungen wie der Digitalisierung und der Industrie 4.0 werden Herstellungsanlagen aber seit den Neunzigerjahren zunehmend mit IT-Infrastrukturen und Office-Netzwerken gekoppelt.

©Sashkin - stock.adobe.com

Immer mehr Schnittstellen zwischen OT und IT sorgen auch im Chemie- und Pharmabereich für eine steigende Anzahl an sensiblen Punkten, an denen auch die Operational Technology von außen angreifbar und verwundbar ist. Zukünftig ist daher zu erwarten, dass Sicherheitslücken hier noch gnadenloser ausgenutzt werden. Besonders Angriffe mit Ransomware (Erpressungssoftware) dürften immer spezieller auf OT-Systeme ausgerichtet werden. Die Angreifer können deutlich mehr finanziellen Druck auf Unternehmen mit systemrelevanten Produktionsanlagen ausüben, auch, weil die Systeme beim Patchen erfahrungsgemäß immer hinterherhängen.

Wertvolle Daten im Visier

OT-Sicherheit umfasst zum einen die Produktionssicherheit und zum anderen die Datensicherheit. Beides hängt miteinander zusammen. Denn die intelligente Vernetzung von Chemieanlagen führt dazu, dass die Produktion ohne digitale Datenströme lahmliegt. Kriminelle Hacker können sich Zugriff auf diese Daten verschaffen und folgendes bewirken: unwiederbringlichen Datenverlust, Datendiebstahl (Spionage) oder Datenverfälschung (Manipulation).

Bis vor einigen Jahren existierten noch keine spezifischen Programme für OT-Systeme, die kontrollieren, ob Daten manipuliert wurden. IT-Programme mussten entsprechend umständlich und aufwendig konfiguriert werden. Daher waren Angriffe mittels Datenmanipulation, die bis hin zum Herunterfahren der OT-Umgebung führen können, das größte Problem. Dies hat sich jedoch geändert: Hacker nehmen gegenwärtig neben Lösegelderpressung die Industriespionage stärker in den Fokus. Dabei lassen sie über Wochen oder Monate unbemerkt Daten abfließen, um diese im Darknet zum Verkauf anzubieten. Von Interesse kann z.B. ein patentgeschütztes Verfahren zur Impfstoffherstellung sein oder Informationen zum Aufbau chemischer Anlagen. Der Datenabfluss kann durch einen berechtigten Zugang eines Mitarbeiters erfolgen – Remote-Zugriffe über VPN-Verbindungen stellen hier eine Herausforderung dar – oder durch unberechtigte Infiltrierung von außen.

Normen schaffen Sicherheit

Nicht alle Chemie- und Pharmaunternehmen gehören zur Kritischen Infrastruktur (KRITIS) nach dem IT-Sicherheitsgesetz 2.0 bzw. der Kritisverordnung des Bundesamtes für Informationstechnik (BSI). Dennoch können viele als systemrelevant bezeichnet werden: Wenn z.B. bei einem Hersteller von Plastikgranulat die Produktion ausfällt, führt dies dazu, dass Lieferketten negativ beeinflusst werden. Bestimmtes medizinisches Werkzeug, wie Spritzen, kann dann nicht mehr hergestellt werden. Der IT-Grundschutz BSI bietet auch für Chemie- und Pharmaunternehmen außerhalb der KRITIS einen wertvollen Leitfaden, um die IT- und OT-Sicherheit zu verbessern.

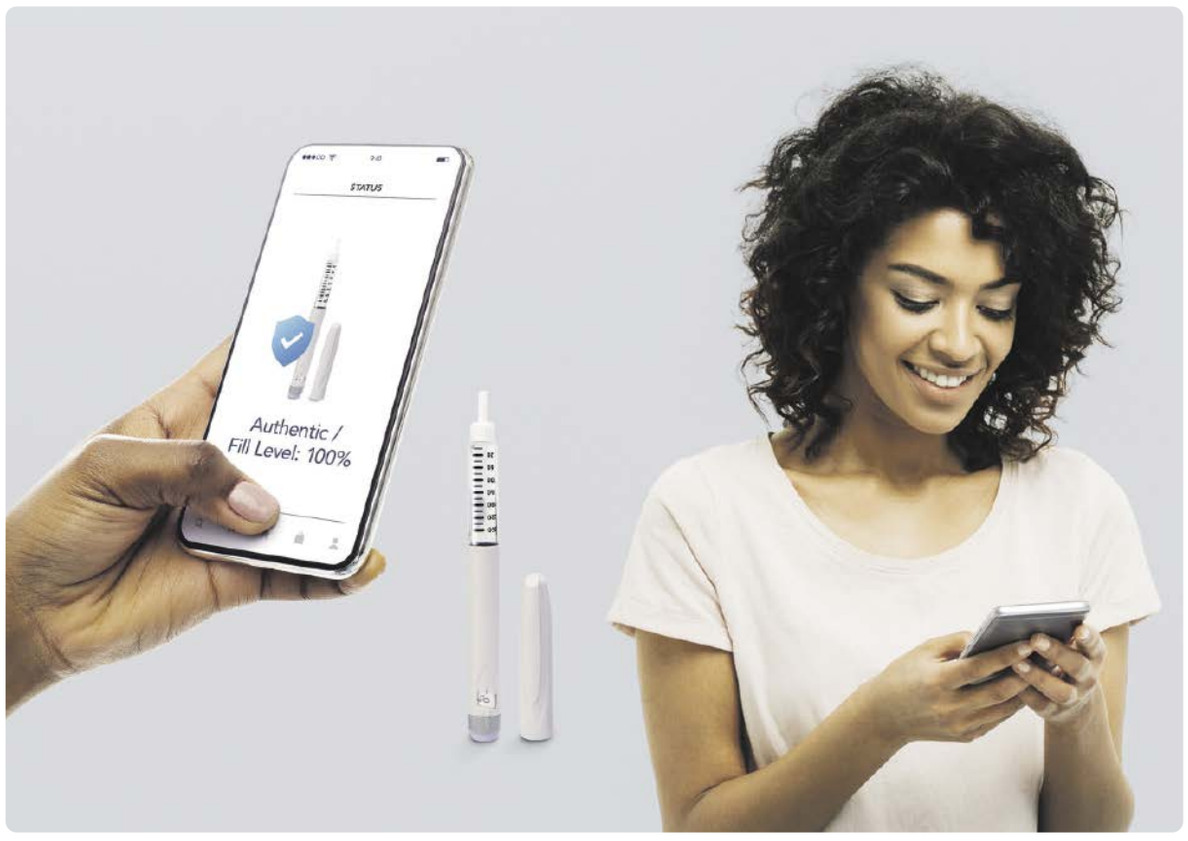
Normen wie die ISO 27001 für Informationssicherheit oder die IEC 62443 für industrielle Sicherheit fordern schon lange einen besonderen Schutz für produzierende Unternehmen. Speziell ausgebildete und zertifizierte Experten können bei der Umsetzung dieser Vorgaben

Fortsetzung auf Seite 35 ▶

Authentifizierung und Manipulationsschutz

Fortschritte in der NFC-Technologie erhöhen nicht nur die Arzneimittelsicherheit

Produktfälschungen stellen Pharmaunternehmen vor Herausforderungen. Darunter leiden Umsatz, Kundenvertrauen und Patientensicherheit. Fortschritte im Bereich der Nahfeldkommunikation (Near Field Communication, NFC) verbessern den Echtheitsschutz und den Erstöffnungsnachweis von Arzneimitteln. In smarten Medikamentenverabreichungssystemen eingesetzt, unterstützt die Technologie zudem das Gesundheitspersonal und die Patienten bei der Umsetzung einer effektiven Medikation.



Die WHO stuft Arzneimittelfälschungen als eine der dringlichsten Herausforderungen für das Gesundheitswesen für die nächsten zehn Jahre ein. Sie schätzt, dass etwa 10 % aller weltweit verkauften Medikamente gefälscht sind. Typische Ziele sind Impfstoffe, Krebsmedikamente und Antibiotika, aber auch stark nachgefragte Produkte wie Vitamine und Nahrungsergänzungsmittel. Mit der zunehmenden Globalisierung der Lieferketten und dem wachsenden Anteil des elektronischen Handels nimmt das Problem weiter zu.

Herkömmliche Methoden der Fälschungsbekämpfung sind oft ineffektiv Um Arzneimittelfälschungen zu bekämpfen, verwenden Pharmaunternehmen in der Lieferkette die Serialisierung auf Artikelebene mit Data-Matrix-Codes. Diese statischen Codes bieten jedoch keinen ausreichenden Schutz vor Fälschungen und decken nicht die „letzte Meile" der Auslieferung an den Patienten ab. Sie erfordern auch eine direkte Sichtverbindung und verfügen nicht über Hightech-Funktionen wie Sensorik.

Mit NFC-Tags versehene Medikamente können über NFC-fähige Geräte digital authentifiziert und mögliche Manipulationen an ihnen erkannt werden. Weltweit sind heute rund 3,4 Mrd. NFC-fähige Geräte, vor allem Smartphones, in Gebrauch. In Echtzeit erhält der Nutzer ein eindeutiges Ergebnis, das ihm anzeigt, ob es sich um ein Originalprodukt handelt. Der Pharmahersteller überwacht Backend-Informationen, um potenzielle Fälschungen oder Graumarkaktivitäten zu identifizieren.

NFC-Tags zur Authentifizierung verfügen neben ihrer eindeutigen Identifikationsnummer über spezielle elektronische Sicherheitsmerkmale. Einige der neuesten Tags sind mit einer sicheren, eindeutigen NFC-Authentifizierungsnachricht (SUN) für die Web-Authentifizierung ausgestattet, die sich mit jedem Auslesen mit einem NFC-Gerät dynamisch ändert. Durch Hinzufügen der eindeutigen ID, eines Zählers und zusätzlicher Daten zu der programmierten NFC-Nachricht, die mit einem kryptografischen Authentifizierungscode geschützt ist, kann nur ein Original-Tag eine gültige SUN-Nachricht generieren. Jeder mit einem solchen smarten E-Tag ausgestatte Artikel kann zuverlässig authentifiziert werden, während seine digitalisierte Erstöffnungsindikation gegen Manipulation geschützt ist.

Sylvia Kaiser-Kershaw, NXP Semiconductors

Durchgängige Transparenz der Lieferkette

Jedes Etikett hat eine eigene, eindeutige Identität und kann über die gesamte Lieferkette hinweg authentifiziert und nachverfolgt werden. Mit Hilfe von Geolokalisierung und cloudbasierter Tracking-Intelligenz lassen sich Fälschungen oder unerlaubte Marktumleitungen leichter erkennen, da jeder – vom Markeninspektor über Arzt oder Apotheker bis zum Verbraucher – die Echtheit und Unversehrtheit des Produkts überprüfen kann.

Darüber hinaus bieten einige Sicherheitsetiketten eine gegenseitige kryptografische Authentifizierungsoption, die sicherstellt, dass nur ein autorisiertes Lesegerät oder ein autorisierter Server auf gespeicherte sensible Etikettendaten zugreifen kann. Produktspezifische Daten können somit in der gesamten Lieferkette vor unerlaubtem Zugriff geschützt werden.

Verankerung von Menschenrechten und Nachhaltigkeit im Lieferkettengesetz

Das ist auch deshalb wichtig, weil am 1. Januar 2023 in Deutschland das Lieferkettensorgfaltspflichtengesetz (LkSG), kurz oft als Lieferkettengesetz bezeichnet, in Kraft tritt. Es verpflichtet Unternehmen mit Niederlassungen in Deutschland, ihre Lieferketten einer Sorgfaltsprüfung im Hinblick auf den Schutz von Menschenrechten und Umwelt zu unterziehen. Bei Verstößen drohen hohe Bußgelder, eine Einschränkung des Marktzugangs und weitere Rechtsfolgen. Eine fälschungssichere Nachverfolgbarkeit liegt somit auch im wirtschaftlichen Eigeninteresse betroffener Unternehmen.

Immer mehr Kunden beziehen zudem ESG-Kriterien in ihre Kaufentscheidungen ein und sanktionieren Anbieter bei Verstößen. So fordert etwa die AOK bei der Ausschreibung von Arzneimittelrabattverträgen von Pharmaherstellern und deren Zulieferern die Einhaltung von Umwelt- und Arbeitsschutzstandards. Wer sie nicht gewährleistet, riskiert Nachteile. Deutsche Pharmaunternehmen arbeiten deshalb seit längerem daran, ihr Lieferkettenmanagement zu verbessern. Maßnahmen wie die Pharmaceutical Supply Chain-Initiative erfordern die Transparenz und Rückverfolgbarkeit, die NFC-Tags ermöglichen.

Zwei Methoden als Erstöffnungsnachweis

Manipulationssichere Etiketten mit einer leitfähigen Verbindung können während der Herstellung auf pharmazeutische Verpackungen aufgebracht werden. Wenn die leitfähige Schleife des Etiketts bricht, wird beim Auslesen mit einem NFC-Gerät die Indikation „geöffnet" unwiderruflich in den Speicher des Tags geschrieben und die Statusmeldung an die Cloud gesendet.

NFC-Tags mit kapazitiver Manipulationserkennung können direkt in Verpackungen wie Flaschenverschlüsse integriert werden, um einen noch besseren Schutz zu bieten. Solche Tags messen die Kapazitätsänderung und vergleichen sie mit vorkonfigurierten Grenzwerten, wenn sie von einem NFC-Smartphone ausgelesen werden. Bei Überschreitung dieser Grenzwerte wird der Status „geöffnet" zur dynamischen SUN-NFC-Meldung hinzugefügt, wodurch die Herstellung der ursprünglichen kapazitiven Struktur des Tags durch einen Betrüger wesentlich erschwert wird.

> *Herkömmliche Methoden der Fälschungsbekämpfung sind oft ineffizient.*

Therapietreue von Patienten erhöhen

Nach Angaben der WHO halten sich in Industrieländern durchschnittlich nur 50 % der Patienten an eine langfristige Medikamenteneinnahme. Oft werden z.B. die Erneuerung eines Rezepts oder die Einnahme einer Dosis vergessen oder Dosierungsanweisungen nicht richtig verstanden. Auch hier können NFC-Tags Abhilfe schaffen.

Durch ihre interaktive Anwendungen unterstützen NFC-Tags die Medikamenteneinnahme und Adhärenz eines Patienten. Angebracht an eine Primärverpackung, wie z.B. Pen oder Autoinjektor, können die Tags einen Link zu Medikamentenanweisungen, Anleitungsvideos und Informationen wie Verfallsdatum oder mögliche Nebenwirkungen aufrufen, wenn man mit einem Smartphone auf diese tippt. Mit einer App können Patienten auch tägliche Erinnerungen für ihre Medikamente einrichten. Über ein „Schloss-und-Schlüssel"-Prinzip können ein nachfüllbares medizinisches Gerät und seine Verbrauchsmaterialien zudem eindeutig einander zugeordnet werden, um die Verwendung von Originalprodukten sicherzustellen. Das Gerät, z.B. ein Injektionsgerät wie ein Insulin-Pen, ist mit einem NFC-Lesegerät ausgestattet, das ein mit einem NFC-Tag versehenes Verbrauchsgut, z.B. eine Patrone, und dessen gespeicherte Daten automatisch und kontaktlos ausliest. Dies erhöht die Patientensicherheit bei Selbstmedikation, reduziert Anwendungs- und Dosierungsfehler, und verhindert den Einsatz von abgelaufenen, falschen oder gefälschten Medikamenten.

Erinnerungsfunktion und Feststellung der Haltbarkeit

Das Lesegerät kann auch aufzeichnen, wann das Medikament eingenommen wurde, und verbunden mit einem Mikrocontroller und einer Displayanzeige in einem medizintechnischen Gerät, den Nutzer benachrichtigen, wenn es bald ersetzt werden muss. Durch eine zusätzliche Bluetooth-Verbindung können die Daten mit dem Mobiltelefon des Patienten synchronisiert oder in der Cloud gespeichert werden, um den individuellen Therapieverlauf zu verfolgen und auf Wunsch Rückmeldungen von einem Arzt zu erhalten.

Die passive NFC-Technologie mit kapazitiver Sensorik kann auch eingesetzt werden, um den Füllstand von Medikamenten in undurchsichtigen Primärverpackungen zu überprüfen und die Patienten via App daran zu erinnern, ihre Vorräte aufzufüllen. Hightech-NFC-Tags mit einem integrierten Sensor, Mikrocontroller und einem großen nichtflüchtigen Speicher unterstützen sogar intelligente Temperaturmessungen: Ein Insulininjektionsstift kann so signalisieren, wenn die Dosis Raumtemperatur erreicht hat, damit die Injektion für den Anwender weniger schmerzhaft ist.

Sylvia Kaiser-Kershaw, Senior Global Marketing Management, Connectivity & Security, NXP Semiconductors

- pr@nxp.com
- www.nxp.com

Zur Person

Sylvia Kaiser-Kershaw ist Senior Global Marketing Manager in der Business Line Connectivity & Security bei NXP Semiconductors. Mit über 20 Jahren Erfahrung in verschiedenen Märkten, darunter Technologie, Konsumgüter, Gesundheitswesen und Vorsorge, ist sie Expertin für die Definition und Umsetzung von Markenstrategien. Sie hat einen MBA-Abschluss von der Webster University und war u.a. in namhaften Kommunikationsagenturen tätig. Bei NXP treibt sie seit 2014 NFC-IoT-Anwendungen voran, die die Interaktion zwischen Marken und Verbrauchern durch digitale Konnektivität, Sicherheit und Intelligenz für physische Produkte verbessern.

Cyberbedrohung in der Operational Technology

◄ Fortsetzung von Seite 34

unterstützen. Auch eine Selbstanzeige beim BSI im Falle eines erfolgten Cyberangriffs auf das eigene Unternehmen darf kein Tabu mehr sein. KRITIS-Betreiber sind dazu sogar verpflichtet. Doch nicht nur für sie empfiehlt sich die Meldung von Hackerangriffen beim BSI. Aus Sicherheitsvorfällen können andere lernen und sich besser schützen. In Zeiten der gestiegenen Bedrohung durch feindlich gesinnte Akteure, die nicht nur einzelne Unternehmen, sondern auch ganze Industrien und Volkswirtschaften schwächen wollen, profitiert davon die Industrie des ganzen Landes.

Maßnahmen

Bei Chemieanlagen geht es oftmals um für Umwelt oder den Menschen gefährliche chemische Stoffe. Unabhängige Safety-Systeme überwachen diesbezüglich bestimmte Grenzwerte und schlagen an, wenn diese überschritten werden. Sie können z.B. das Austreten giftiger oder umweltschädlicher Chemikalien verhindern. Auch Löschsysteme oder ein roter Notfallschalter, der manuell betätigt werden muss, gehören in diese Kategorie.

> *Hacker nehmen gegenwärtig neben Lösegelderpressung die Industriespionage stärker in den Fokus.*
>
> Patrick Latus, Mod IT Services

Solche Systeme dürfen nicht mit der Operational Technology oder der IT gekoppelt sein, denn sie müssen komplett unabhängig von anderen Systemen funktionieren. Sie sollten regelmäßig auf das ordnungsgemäße Funktionieren geprüft werden.

Unternehmen, die bei der Security noch Nachholbedarf haben, sollten damit nicht länger warten. Ein erster Schritt ist bei vielen die Dokumentierung der Assets. Nur wenige OT-Betreiber haben einen genauen Überblick über alle Systeme. Unverzichtbar ist auch das systematische und kontinuierliche Scannen auf Schwachstellen mittels professioneller Software. Firewalls, Antivirus-Komponenten, Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) müssen eingerichtet werden und danach jederzeit auf neuestem Stand gepatcht sowie korrekt konfiguriert werden. Da neue Patches häufig auch Systemkomponenten lahmlegen oder gar zum Ausfall von Systemen führen können, ist hier detaillierte OT-Fachexpertise gefragt.

Hilfreich ist häufig der Austausch unter Kollegen und die Recherche nach existierenden Workarounds, die schon funktionieren.

Mit solchen Behelfslösungen können gerade im Bereich Operational Technology kritische Sicherheitslücken geschlossen werden. OT-Security ist aufgrund der Komplexität und Einzigartigkeit der Systeme ein noch langwierigerer und kleinteiligerer Prozess als IT-Security. Er muss in kleinen Schritten gegangen werden.

Patrick Latus, OT-Sicherheitsexperte, Mod IT Services, Einbeck

- p.latus@it-mod.de
- www.it-mod.de