www.laborpraxis.de | Februar 2022 | 46. Jhg. | 19,90 € | LP 1/2

LABOR PRAXIS

WER UNS NUTZT ... EHR.

Zurück in die Zukunft der Laborsicherheit > S. 22

Neues Sicherheitskonzept für HPLC-Lösungsmittel

MIKROFLUIDIK

Molekularer Fingerabdruck erkennt verborgene Krebserkrankungen > S. 14 //

LABORTECHNIK

Das sind die GMP-Anforderungen an die Messgeräte-Software > S. 26 //

LABORAUSSTATTUNG

Vier Kriterien für eine kontaktlose Labor-Zugangskontrolle > S. 42 //

VOGEL COMMUNICATIONS GROUP

Bild: Elatec

1 Mit einer Chipkarte lassen sich Zugriffsrechte zu Laboren individuell vergeben.

Sicherheit mit System

Kontaktlose Authentifizierung für Labore // In Laboren und Reinräumen dürfen nur Befugte Zutritt haben, um Menschen, Maschinen und Daten zu schützen. Eine Authentifizierungslösung muss den besonderen Anforderungen dieser Umgebung gerecht werden. Vier Kriterien sind dabei besonders zu beachten.

BURHAN GÜNDÜZ*

Die Arbeit in Laboren und Reinräumen erfordert von den Mitarbeitern besondere Kenntnisse – sowohl in Bezug auf den Umgang mit den kostspieligen und sensiblen Geräten sowie den empfindlichen oder gesundheitsgefährdenden Materialien, als auch im Hinblick auf die strengen Hygienevorschriften. Aber auch externe Dienstleister wie Reinigungskräfte müssen die hier geltenden Regeln einhalten. Je höher die Schutzstufe oder die Reinraumklasse, desto strenger sind die Sicherheitsvorgaben. Für Betreiber bedeutet das: Sie müssen gewährleisten, dass nur autorisierte und geschulte Personen Zutritt zu den Räumen und Zugang zu Anlagen und Systemen erhalten.

* B. Gündüz,
Elatec, 82178 Puchheim,
Tel. +49 89 552 9961-0

Eine weitere zentrale Herausforderung ist die Systemsicherheit: Es gilt, Maschinen, Anlagen und Peripheriegeräte ebenso wie sensible und wertvolle Daten wirksam vor unbefugtem Zugriff zu schützen.

Benutzer sicher und einfach authentifizieren

Ein modernes Benutzerauthentifizierungs- und Zugangskontrollsystem auf Basis von RFID, das auch

den Einsatz mobiler Berechtigungsausweise erlaubt, ist eine einfache und sichere Lösung, um Personen, Daten und Inventar zu schützen. Darüber hinaus bietet es die Möglichkeit, die Prozesse zuverlässig und mit geringem Aufwand zu dokumentieren. So werden beispielsweise Qualitätsmanagement und Arbeitszeiterfassung erheblich erleichtert.

Eine ebenso unkomplizierte wie günstige Option der Benutzerauthentifizierung und Zugangskontrolle ist ein Ausweis, der mit einem RFID-Tag ausgestattet ist – und den die meisten Mitarbeiter in Form einer ID-Karte oder eines Tokens bereits bei sich tragen. Auch der Einsatz von Wearables, beispielsweise Armbänder, ist möglich. Wird ein solcher physischer Ausweis an das Lesegerät gehalten, erfolgt der Identifizierungsprozess automatisch. Die autorisierte Person erhält umgehend Zutritt zu den Laborräumen und kann auf Computersysteme oder Anlagen zugreifen. Je nach Qualifikation der Mitarbeiter lassen sich die Berechtigungen dabei individuell anpassen.

Möglich ist auch der Einsatz von digitalen Berechtigungsnachweisen, so genannte mobile Credentials. Sie basieren auf den Technologien Near Field Communication (NFC) oder Bluetooth Low Energy (BLE), mit denen ein Großteil aller Smartphones ausgestattet ist. Der internationale Übertragungsstandard NFC erlaubt den kontaktlosen und gesicherten Austausch von Daten auf kurzer Distanz. Die Transaktion wird also abgewickelt, wenn sich das Smartphone in der Nähe eines Multifrequenz-Lesegeräts befindet. Bei der Funktechnik BLE hingegen muss das Handy für den Authentifizierungsprozess nicht mehr zwingend aktiv an das Lesegerät gehalten werden – je nachdem, welche Distanz im System festgelegt ist. Sowohl physische als auch digitale Berechtigungsnachweise erlauben eine komfortable, berührungslose und damit hygienische Authentifizierung. Erfordert das Arbeitsumfeld außerdem eine Zwei-Faktor-Authentifizierung, kann RFID in Verbindung mit biometrischen Systemen wie einem Armband oder Passwortsystemen verwendet werden.

Vier Kriterien für die Wahl des richtigen Readers

Das Herzstück eines modernen Zutritts- und Zugangskontrollsystems sind universelle Lesegeräte. Gerade für den Gebrauch in Laboren und Reinräumen müssen sie spezifische Anforderungen erfüllen – auch um sicherzustellen, dass gesetzliche Standards eingehalten werden. Folgende vier Aspekte sind bei der Auswahl zu beachten:

1. Hygiene – Die besonderen Anforderungen von GMP (Good Manufacturing Practice) -Umgebungen werden im Hinblick auf die verwendeten Reader häufig vernachlässigt. Geräte, die in herkömmliche Kunststoffgehäuse eingebaut sind, können nicht regelmäßig mit Desinfektions- oder Reinigungsmitteln behandelt werden. Der Grund: Die Gehäuse nehmen bei der Verwendung aggressiver Substanzen und häufigen Reinigungszyklen leicht Schaden. In Reinräumen kann das sogar die Arbeitsergebnisse beeinträchtigen, denn ein angegriffenes Gehäuse birgt die Gefahr, dass freigesetzte Partikel die Umgebung kontaminieren. Es empfiehlt sich daher der Einsatz von Lesegeräten, die in ein Gehäuse aus Edelstahl und Glas integriert sind, also Materialien, die üblicherweise für GMP-Anwendungen verwendet werden. Sie halten den strengen Reinigungs- und Hygieneanforderungen stand. Die Gehäuse sollten ohne Ecken, Kanten oder offene Anschlüsse konzipiert sein und der Schutzklasse IP65 entsprechen (Schutz gegen Niederdruck-Strahlwasser aus allen Richtungen sowie gegen Kondenswasser und Spritzwasser).

2. Sicherheit von Daten, Systemen und Personen – Beim Zutritt zu Räumlichkeiten sowie dem Zugang zu Computernetzwerken und Softwaresystemen erfordern Labor- und Reinraumumgebungen ein hohes Maß an Sicherheit. Das bedeutet, dass die verwendeten Lesegeräte sowohl gegen physische Manipulationen als auch gegen Hackerangriffe resistent sein müssen. Lesegeräte, die sich für Hochsicher-

LP Tipp+
mehr zum Thema:

- Mehr zu diesem Thema finden Sie auf www.laborpraxis.de, Stichwort: **RFID**
- **Fallbeispiele** für den EInsatz von RFID-Zugangslösungen – etwa in der Medizintechnik – gibt es unter www.elatec-rfid.com/de-de/alle-fallbeispiele

Bild: Elatec

2 Reinräume unterliegen strengen Zugangsbeschränkungen. Auch hier können Keycards mit RFID-Technik die Zugriffsrechte unkompliziert regeln.

heitslabore oder Produktionsumgebungen eignen, sollten eine fortschrittliche Verschlüsselungstechnologie unterstützen. Verschlüsselte RFID- oder BLE-/NFC-Signale sind schwerer abzufangen oder zu fälschen. Für zusätzliche Sicherheit sorgen Lesegeräte, die mit biometrischen Verfahren (Wrist-Band) für eine Zwei-Faktor-Authentifizierung kompatibel sind. Nicht zuletzt gilt es, die Mitarbeiter durch eine Zutrittskontrolle zu schützen. Denn in Laboren und Reinräumen wird mit Materialien gearbeitet, die bei unsachgemäßer Nutzung eine erhebliche Gesundheitsgefahr darstellen können.

3. Flexibilität – Weltweit sind Dutzende RFID-Kartentechnologien im Einsatz, jede mit ihren eigenen Datenformaten, Kommunikationsfrequenzen und Sicherheitsfunktionen. Die Karten können grob in Hochfrequenz (HF) und Niederfrequenz (LF) unterteilt werden, je nach Frequenzbereich, den sie für die Kommunikation nutzen. Innerhalb dieser Kategorien haben die Karten der verschiedenen Hersteller jedoch ihre eigenen, einzigartigen Formate. Unternehmen mit mehreren Standorten oder bereits vorhandenen Benutzerauthentifizierungs- und Zugangskontrollsystemen sollten auf universelle Lesegeräte setzen, die für den weltweiten Einsatz zertifiziert sind und eine Vielzahl an Technologien unterstützen. Sie bieten eine vergleichsweise einfache All-in-One-Lösung, die hilft, Zeit und Kosten zu sparen. Eine gute Wahl sind beispielsweise Reader-Modelle des RFID-Anbieters Elatec, die bis zu 60 gängige Transpondertechnologien verarbeiten können. Mulitfrequenz-Lesegeräte erlauben es, alle aktuell und in Zukunft im Unternehmen eingesetzten Transpondertechnologien zu verarbeiten und sind auch für die Smartphone-Authentifizierung mit BLE- oder NFC-Technologie geeignet.

4. Zukunftssicherheit – Änderungen an Betriebssystemen, der Einsatz neuer Transpondertechnologien oder aufkommende Sicherheitsbedrohungen können es erforderlich machen, Lesegeräte zu aktualisieren oder neu zu konfigurieren. Es empfiehlt sich, Lesegeräte zu implementieren, die über eine offene Programmierschnittstelle verfügen. Damit sind die Geräte bei sich ändernden Anforderungen maximal anpassungsfähig und zukunftssicher, denn es lassen sich jederzeit Updates und Upgrades durchführen. Wichtig dabei: Diese sollten sich via Fernwartung vornehmen lassen. So kann vermieden werden, dass Techniker jedes einzelne Gerät aufwändig ausbauen, anpassen und wieder einbauen müssen. Außerdem sollten Lesegeräte so programmierbar sein, dass sie spezifische Funktionen für anspruchsvolle PC-Anmeldesoftware ermöglichen und mobile Zugangskontrolltechnologien unterstützen. So erfüllen die Lesegeräte die Bedürfnisse von Labor-Betreibern und Benutzern über einen langen Zeitraum. ■

LP Info

Christian Lüttmann, Redakteur

SO FUNKTIONIERT RFID

RFID-Karten haben einen eingebetteten Chip (oder Tag), der aus **zwei Hauptkomponenten** besteht:

- einer integrierten Einheit, die **Informationen speichern und verarbeiten** kann
- einer Antenne zum **Senden oder Empfangen** eines Signals

Auf jeder RFID-Karte ist ein **eindeutiger Datensatz** – beispielsweise eine Nummer – gespeichert, der zur Identifizierung der Karte und damit auch der Person dient, die sie bei sich trägt. Befindet sich eine RFID-Karte in der Nähe eines Lesegeräts, sendet dieses ein Funksignal aus, um den Datensatz abzufragen. So wird der Tag aktiviert, der dann die Energie des Funksignals nutzt, um dem Leser seine ID mitzuteilen.