Foto: Istock.com – PeopleImages

Ein Zutritts- und Zugangskontrollsystem muss unter anderem sicherstellen, dass auch der logische Zugang zu Dateien und Systemen nach unterschiedlichen Berechtigungslevel möglich ist.

Clever auf den Campus

Moderne Authentifizierung auf Basis von RFID und Smartphones ermöglicht es Hochschulen, allen Berechtigten adäquat Zugang zu geben.

BURHAN GÜNDÜZ

Die vielfältigen Personengruppen an Hochschulen stellen eine Herausforderung in puncto Sicherheit dar: Auf dem Campus bewegen sich zahlreiche Menschen; sie alle gehen unterschiedlichen Tätigkeiten nach und haben einen individuellen Tagesablauf. Entsprechend benötigen sie Zutritt zu verschiedenen Räumlichkeiten und Einrichtungen auf dem Gelände – vom Studierendenwohnheim über die Bibliothek bis hin zu Büros. Und das am besten kontaktlos und damit hygienisch. Um diese Komplexität abbilden zu können, ist technische Unterstützung notwendig. Diese bietet ein modernes, einheitliches Zutritts- und Zugangskontrollsystem. Es stellt sicher, dass ausschließlich berechtigte Personen Räume betreten können und Zugriff auf Dienste oder schützenswerte Informationen erhalten.

Zutritt und Zugang einfach unter Kontrolle

Ein Zutritts- und Zugangskontrollsystem muss eine Reihe von Anforderungen erfüllen, damit es dem komplexen Bedarf von Hochschulen gerecht wird. So ist etwa der Nutzerkomfort essenziell: Der Authentifizierungsprozess sollte für die Anwender ebenso einfach wie komfortabel ablaufen und Berührungspunkte minimieren – ein Aspekt, welcher durch die Pandemie in den letzten Jahren deutlich an Bedeutung gewonnen hat. Im Idealfall deckt eine Lösung alle Anwendungen ab, die die verschiedenen Nutzergruppen im Unialltag benötigen. So können Studierende beispielsweise Spinde und Drucker nutzen, in der Bibliothek Arbeitsplätze buchen, die den Abstandsregeln entsprechen oder hochschuleigene Sportstätten besuchen. Mitarbeiter und Dozenten erhalten, abhängig von ihrer Rolle, weitergehende Berechtigungen. Diese können es ihnen erlauben, Parkplätze zu nutzen, im Labor zu arbeiten und sich mit Single Sign-on mit einem individuellen Berechtigungslevel im Hochschulnetzwerk anzumelden – um nur einige Optionen zu nennen.

„Multifrequenz-Lesegeräte bieten maximale Flexibilität. Sie sind mit bis zu 60 weltweit gängigen Transpondertechnologien kompatibel."

Burhan Gündüz, Vice President Secure Printing EMEA & Japan.

Sicherheit und Flexibilität

Während „Komfort" das entscheidende Stichwort für die Nutzer ist, zählen für Hochschulleitung und Campus-IT bei einer Zutritts- und Zugangskontrolle weitere wichtige Aspekte. Hier steht vor allem das Thema Sicherheit von Personen, Gebäuden, Anlangen und der Schutz von Daten im Fokus. Darüber hinaus sind Flexibilität und Zukunftsfähigkeit des Systems gefragt. Es soll kompatibel mit bestehenden Lösungen auf dem Gelände sein, Anpassungen an sich ändernde Anforderungen und gesetzliche Vorgaben erlauben und künftige Technologien verarbeiten können. Zudem muss die Verwaltung der Berechtigungen von der Erteilung bis zur Sperrung so einfach wie möglich umsetzbar sein.

Studierende haben die Wahl

Eine moderne Authentifizierungslösung arbeitet auf der Basis von RFID und digitalen Berechtigungsnachweisen. Die sogenannten mobilen Zugangsberechtigungen nutzen die Technologien NFC (Near Field Communication) oder BLE (Bluetooth Low Energy), mit denen ein Großteil aller mobilen Endgeräte ausgestattet ist. So können sowohl eine RFID-Karte als auch ein Smartphone als kontaktlose Identifikationsmedien dienen – einfach an das Lesegerät halten und schon ist der Weg für autorisierte Personen frei.

Vor der Umsetzung einer einheitlichen Campus-Lösung ist jedoch zunächst die Frage zu klären, welche Technologie zur Authentifizierung eingesetzt werden soll. Denn sowohl RFID-Karten als auch mobile Zugangsberechtigungen bieten Vorteile für die Nutzung im Hochschulumfeld. So sind ID-Karten in Form von Studierenden- und Mitarbeiterausweisen an vielen Hochschulen bereits im Einsatz und lassen sich für Anwendungen eines Zutrittskontrollsystems nutzen. Als Innovationstreiber sollten Hochschulen jedoch auch die Chancen der digitalen Transformation nutzen – nicht nur in der Lehre, sondern auch auf dem Campus. In diesem Umfeld sind Smartphones ein optimales Identifikationsmedium. Zum einen ist das Handy für Lernende und Lehrende ständiger Begleiter im Alltag, sodass sie Berechtigungsnachweise auf dem Smartphone immer griffbereit haben – und anders als Studierendenausweise in aller Regel nicht weitergeben. Zum anderen spart die zentrale und einfache Verwaltung der mobilen Berechtigungen Ressourcen bei der Campus-IT. Maximale Flexibilität bietet eine hybride Lösung, die den parallelen Einsatz von Karten und Smartphones für die Authentifizierung erlaubt. So kann die Entscheidung für ein Identifikationsmedium individuell für jede Anwendung und Person getroffen werden und lässt sich bei Bedarf einfach anpassen.

Foto: Elatec

Für die Zugangsberechtigungen werden die Technologien NFC oder BLE genutzt, mit denen ein Großteil aller mobilen Endgeräte ausgestattet ist.

Schutz von Personen und Daten

Damit der zuverlässige Schutz von Personen, Gebäuden, Anlagen und Daten gegeben ist, müssen die verwendeten Lesegeräte gegen physische Manipulationen ebenso wie gegen Hackerangriffe gerüstet sein und eine fortschrittliche Verschlüsselung unterstützen. Nur dann bieten sie das für den Authentifizierungsprozess erforderliche Maß an Sicherheit. Um eine RFID-basierte Authentifizierungslösung effektiv und ganzheitlich abzusichern, reicht eine Betrachtung des Lesegerätes allein jedoch nicht aus. Es ist notwendig, das komplette System in die Sicherungskonzepte des Unternehmens einzubeziehen.

Zukunftssicherheit der Zutrittslösung dank zentraler Fernwartung

Anforderungen und IT-Infrastrukturen verändern sich im Laufe der Zeit und machen Anpassungen erforderlich. Nur mit einem flexiblen System, das Optimierungen, Adaptionen und Upgrades vorsieht, sind Hochschulen auch in Zukunft auf der sicheren Seite. Denn auf einem Campus befinden sich hunderte Lesegeräte, die über das oft weitläufige Gelände oder sogar verschiedene Standorte verteilt sind. Normalerweise müssten Updates von einem Techniker aufwendig auf jedes einzelne Gerät direkt vor Ort aufgespielt werden. Sind Remote-Updates möglich, können hingegen alle installierten Lesegeräte unabhängig von ihrem Standort problemlos und zeitsparend von zentraler Stelle aktualisiert werden. ■

Burhan Gündüz, Vice President Secure Printing EMEA & Japan.

ELATEC GmbH:
www.elatec.com