Ergonomische und sichere Zutrittssteuerung

Die Zutrittssteuerung wird immer sicherer und ist in Verbindung mit anderen IT-Systemen oder biometrischen Lösungen auch komplexer geworden.

Diese Systeme zur Zutrittssteuerung schützen nicht nur vor unberechtigten Zutritt von Personen zu sensiblen Bereichen, sondern dienen zunehmend auch dem Gesundheits- und Arbeitsschutz der Mitarbeiter. Wurde bislang besonders auf Sicherheit, Funktionalität und Kosten bei der Beschaffung geachtet, ist jetzt auch die Benutzerfreundlichkeit und Akzeptanz ein Auswahlkriterium.

Zutrittsperipherie – Klassifizierung nach Sicherheitsgrad

Bei der Planung und Auswahl des Zutrittssystems sind am Einsatzort viele Einflussfaktoren zu beachten (siehe Bild 1). Dazu gibt die Norm EN 60839-11-1 vier Sicherheitsgrade vor, von niedrig (= 1, z.B. für Hotels) bis hoch (= 4 für Hochsicherheitsbereiche). Die Einstufung in eine der vier Sicherheitsgrade nimmt der Betreiber nach seinen Forderungen und einer zuvor durchgeführten Risikoanalyse vor, ggf. gemeinsam mit dem Anbieter. Bedeutsam ist dabei die Abwägung zwischen Kosten, Sicherheitsgrad und Erkennungsgeschwindigkeit an der Zutrittsstelle.

Abb. 1: Einflussfaktoren für die Auswahl der Zutrittsperipherie am Einsatzort

Bei niedrigen bis mittleren Sicherheitsanforderungen erfolgt die Personenerkennung mittels RFID-Ausweis. Alternativ können digitale Firmenausweise auf ein Smartphone übertragen und genauso genutzt werden. Besonders an Eingängen mit einer hohen Nutzerfrequentierung ist eine schnelle Prüfung der Zutrittsberechtigung unerlässlich. Denn „Schlange stehen" am Werkseingang möchte kein Arbeitnehmer. Die Personenidentifikation kann quasi im „Vorbeigehen" erfolgen, dabei ist lediglich der Datenträger (RFID-Ausweis/Transponder oder Smartphone) im Abstand von wenigen Zentimetern vor das Lesegerät zu halten.

Beim Zutritt zu einem Rechenzentrum mit sensiblen Daten oder zu militärischen Einrichtungen sollte die Erkennungsgeschwindigkeit keine große Rolle spielen. Die sehr hohen Sicherheitsanforderungen können dem Sicherheitsgrad 4 zugeordnet werden. Hier gibt es wenige Alternativen zum Einsatz von biometrischen Systemen und der Mehrfaktor-Authentifizierung, denn andere Methoden erfüllen nicht die Anforderungen an die Manipulations- und Fälschungssicherheit.

Benutzerfreundliche und sichere Zutrittsstellen erhöhen die Akzeptanz

Die Berücksichtigung hygienischer und ergonomischer Aspekte soll dem Schutz und der Zufriedenheit von Arbeitnehmern dienen. Dabei ist es wichtig, die Variabilität des Menschen (z.B. dessen Größe) und die Einsatzbedingungen (Eingangsbereich/Fertigung/Büro) in der Gestaltung zu berücksichtigen. Dies hat Auswirkungen auf bauliche Maßnahmen an der Zutrittsstelle.

So kann es ein Gebäude- und Raumzugang oder eine Flucht- und Rettungswegtür sein, die Anforderungen an Brand- und Einbruchschutz sowie Barrierefreiheit erfüllen muss. Insbesondere an Eingängen sind Zutrittsleser die Visitenkarte eines Unternehmens. Sie geben dem Besucher beim Zutritt von Gebäuden Rückschlüsse auf ein aktives Sicherheitsbewusstsein mit Anwendung moderner Technologien und einen ersten Eindruck von der Unternehmenskultur.

Am kostengünstigsten sind autonome, batteriebetriebene, mechatronische Schließzylinder und Tür-Terminals, die keine Verkabelung erfordern und auch noch nachträglich in Türen eingebaut werden können. Entsprechen die Anforderungen dem Sicherheitsgrad 1, können z.B. Büro- oder Hotelzimmertüren mit elektronischen Offline-Türbeschlägen abgesichert werden. Die Berechtigungsprüfung für den Zutritt erfolgt hierbei mittels PIN-/Ausweiseingabe oder Fingerprint und aktueller Systemzeit. Die Türbeschläge sind in allen gängigen Türschild- bzw. Rosettenvarianten und für Vollblatt-, Rohrrahmen- und Glastüren verfügbar.

Komfortabler und ein breiteres Einsatzspektrum bieten vernetzte Zutrittssysteme mit einer übergeordneten Zutrittszentrale, an der abgesetzte Ausweis-/biometrische Leser und Vereinzelungseinrichtungen angeschlossen werden können. Dabei ist die mögliche Anzahl und Art der Vernetzbarkeit (per Funk oder verkabelt), der anzuschließenden Zutrittsgeräte zu beachten. Häufig werden mechatronische Schließsysteme mit vernetzten Online-Zutrittssystemen mittels eines virtuellen Netzwerks (z.B. „NetWorkOnCard“) kombiniert.

Hierbei werden tagesaktuelle Zutrittsrechte am Zeiterfassungsterminal auf den RFID-Mitarbeiterausweis geschrieben. Somit können verschiedene Zutrittsstellen (Türen, Tore, Schleusen etc.) in einem Gebäude – ihrer Hierarchie entsprechend – auch unterschiedlich gesichert werden. Vernetzte Zutrittssysteme sind meist auch Teil eines integralen Sicherheitskonzepts mit Alarmanlagen, Videoüberwachung, Einbruchmeldesystemen und zentraler Leittechnik.

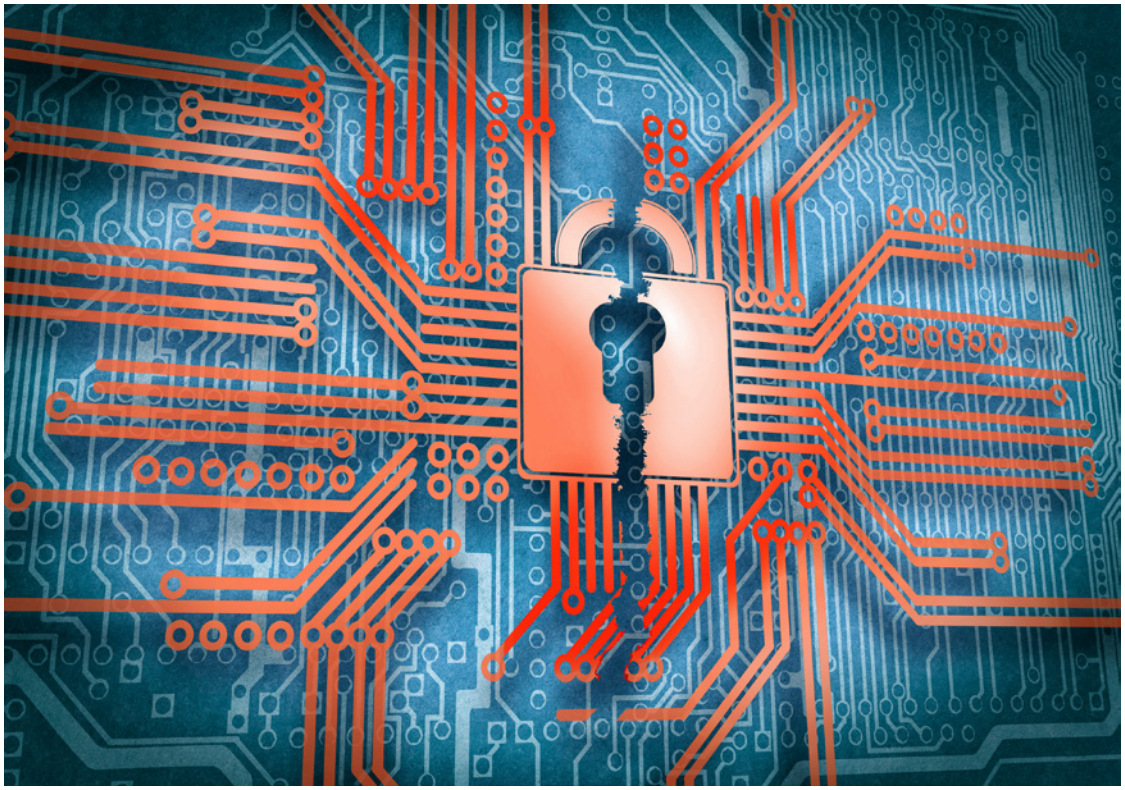
Für die Zutrittsleser sind unter ergonomischen Gesichtspunkten auch die Befestigungsmöglichkeiten wie Wand- oder Säulenmontage zu berücksichtigen. Sie sollen möglichst flach an der Wand oder einer Säule befestigt sein, nicht zu weit herausstehen, um kein Hindernis darzustellen oder gar Verletzungen zu verursachen. Auch schmale Leser-Varianten, für die Montage an Türrahmen oder Zargen, sind zu berücksichtigen (siehe Abb. 2).

Die Zutrittsleser müssen in einer bequemen Haltung und kontaktlos genutzt werden können. Dabei sind die unterschiedlichen Körpergrößen der Mitarbeiter bei der Montagehöhe zu beachten. Durch Einsatz von Signalgebern wird die Bedienerführung optisch unterstützt, beispielsweise kann eine Fehllesung durch Rot-Signalisierung kommuniziert werden. Die Bedienung muss selbsterklärend und nutzerfreundlich sein.

Abb. 2: Eine schlanke Bauweise des Zutrittslesers erlaubt die Befestigung an schmalen Montagestellen (Foto: PCS Systemtechnik).

Biometrische Systeme – hochsicher und komfortabel

Stark ansteigend ist die Nachfrage nach biometrischen Systemen, nicht nur als Hochsicherheitslösung, vielmehr auch aus ergonomischen, hygienischen und Komfort-Gründen. Diese Erkennungsverfahren sollen die Schwachstellen anderer Identifikationsmethoden, wie vergessene oder ausgespähte PIN und verlorene, gestohlene bzw. beschädigte Ausweise, ausgleichen oder ergänzen. PIN, Ausweis und biometrische Daten sind aber keine Gegensätze, sondern können sich ergänzen. Je nach gewünschter Sicherheitsstufe können diese Technologien für eine Mehrfaktor-Authentifizierung kombiniert werden.



Bei der Systemauswahl sind viele Einflussfaktoren zu beachten wie die Umgebungsbedingungen, der Risikograd, die Nutzeranzahl, der Datenschutz und die Akzeptanz bei den Anwendern. Bei der Prüfung der Übereinstimmung der biometrischen Merkmale ist eine Toleranzschwelle anzuwenden. Hierbei ist zwischen False Acceptance Rates (FAR), „Akzeptanzraten für falsche Erkennungen" sowie False Rejection Rates (FRR), „Rückweisungsraten für falsche Erkennungen" zu unterscheiden. Die Wahrscheinlichkeit der Falschakzeptanz und der Falschrückweisung müssen in einem akzeptablen Verhältnis zum Sicherheitsniveau stehen.

Seminarhinweis

Im Seminar „Zutrittssteuerung und Identifikationsmanagement", am 28.9. bis 29.9.2023 in Hünfeld bei Fulda, beim Bundesverband Sicherheitstechnik e.V. (BHE), werden neben der Beschreibung der technischen Komponenten die wichtigen Bereiche Personenidentifikation, Planung, Projektierung, Installation, Inbetriebnahme und Instandhaltung von Zutrittssteuerung erläutert. Die Darstellung der Vortragsinhalte erfolgt vollkommen hersteller- und produktneutral. Selbstverständlich werden bei der Seminardurchführung auch die vorgeschriebenen Hygieneregeln beachtet und umgesetzt.
Hinweise zum Seminar können abgerufen werden unter:
https://www.bhe.de/weiterbildung/programm/zutrittssteuerung-und-identifikationsmanagement-4.

Beim Einsatz solcher Systeme ist die Datenschutz-Grundverordnung (DS-GVO) zu beachten, dazu gehören die ausdrückliche Einwilligung der Nutzer und die Dokumentation mit dem Nachweis des berechtigten Einsatzes biometrischer Systeme. Die Erforderlichkeit ergibt sich, wenn alternative Zutrittssysteme (z.B. mit Ausweis und PIN) nicht die erforderliche Sicherheit hinsichtlich der Verhinderung eines unbefugten Zutritts erzielen, z.B. beim Zutritt zu einem Rechenzentrum mit besonders sensiblen (personenbezogenen) Daten.

Der Fingerprint war bisher das bekannteste und weitverbreitetste Identverfahren. Zur Personenidentifikation genügt ein einfaches Auflegen des Fingers auf dem Sensor. Leider ist die Technik nicht ganz unproblematisch, denn Fingerabdrücke können mit moderatem Aufwand kopiert und dupliziert werden.

Im laufenden Betrieb kommt es immer wieder vor, dass bei einzelnen Personen der Fingerabdruck nicht erkannt wird. Die Gründe dafür sind vielfältig: zu trockene Haut, Nässe bzw. Kälte aber auch falsches Auflegen des Fingers und Verschmutzungen der Haut oder des Sensors. Schwach ausgeprägte Minutien (d.h. die Endpunkte und Verzweigungen der Hautrillen auf dem Finger) beeinträchtigen das Leseergebnis. Eine hohe Fehlerquote führt zu einer zunehmenden Ablehnung.

Nicht nur in Zeiten der Pandemie wird die kontaktbehaftete Nutzung unter Hygiene-Aspekten kritisch gesehen. Abhilfe für eine bessere Akzeptanz schafft hier die regelmäßige Reinigung des Sensors mit einem feuchten (nicht nassen), nicht kratzenden Tuch. Geeignet sind Wattestäbchen, Mikrofaser- und Brillenputztücher. Alternativ werden aber auch Systeme angeboten, bei denen der Finger mit einer Kamera dreidimensional und berührungslos erfasst wird.

Bei einem 3D-Fingerprint-Scanner muss man keine Finger auflegen, sondern lediglich seine Hand kontaktlos über einen Sensor streichen. In dieser Wink-Bewegung werden vier Finger in weniger als einer Sekunde gescannt und verifiziert, und damit ist das System ideal für Anwendungen mit einem hohen Durchsatz geeignet.

Eine weitere, sehr sichere biometrische Lösung ist die Iriserkennung. Aber diese hat sich nie flächendeckend durchgesetzt, da ein Durchleuchten des menschlichen Auges als nicht angenehm wahrgenommen wird. Viele stationäre Systeme haben den Nachteil, dass eine sorgfältige Positionierung des Nutzers erforderlich ist. Auch die Hygiene wird oft als Einwand erwähnt, da Benutzer in stationären Systemen ihr Kinn auf einen Halter legen müssen, der bereits von vielen Menschen verwendet wurde. Eine bessere bis hohe Benutzerakzeptanz ergibt sich nur durch kontaktfreie, verlässliche und hygienische Erfassung der biometrischen Merkmale, wie sie z.B. bei der Gesichts- und Handvenenerkennung gewährleistet wird.

Die Gesichtserkennung nimmt im Alltag eine immer größere Rolle ein: z.B. für Einlasskontrollen am Flughafen oder zum Log-in beim PC oder Smartphone, statt PIN oder Passwort. Bei diesem Verfahren wird mittels 2D-, Infrarot- und/oder 3D-Kamera automatisch ein Gesichtsbild der zu identifizierenden Person aufgenommen und mit einem vorher abgespeicherten und ähnlich produzierten Bild verglichen. Nachdem die Kamera das Gesicht mit Augen, Nase und Mund aufgenommen hat, wertet das Erkennungssystem die geometrischen Proportionen, die diese Merkmale zueinander aufweisen, aus.

Diese Technologie ist mittlerweile so weit entwickelt , dass eine Gesichtserkennung auch bei Dunkelheit, starker Sonneneinstrahlung oder bei reflektierendem Sonnenlicht möglich ist. Mit einer Identifikationszeit von unter einer Sekunde kann ein hoher Personendurchsatz erreicht werden. Inzwischen tolerieren solche Systeme auch Veränderungen des Gesichts, z.B. durch Brille, Bart, Mütze oder Mund-Nasen-Schutz.

Aus Sicht des Datenschutzes wird diese Technologie, aber auch ihre Nutzer, besonders kritisch gesehen. Ein sehr großes Problem ist hier der mögliche Identitätsmissbrauch durch die Erlangung der entsprechenden biometrischen Daten (Gesichtsbilder). Beispielsweise gibt es berechtigte Sorgen vor einem flächendeckenden Netz von Überwachungskameras, die Personen identifizieren können. Viele Datenbanken, z.B. in sozialen Netzwerken, sind mit Passbildern gefüllt, die eine schnelle Personenzuordnung ermöglichen. In keinem Fall dürfen die Risiken der Gesichtserkennung unterschätzt werden.

Bei den Nutzern gibt es oft Vorbehalte gegenüber biometrischen Lösungen aufgrund fehlender, missverständlicher oder falscher Informationen. Für die objektive Aufklärung und Information über solche Systeme können Hersteller, Verbände und Anwender nie genug tun. Der Bundesverband Sicherheitstechnik e.V. (BHE) möchte hier durch sein Informationsangebot wie White-Papers, Praxisratgeber und Seminare (siehe: https://www.bhe.de/seminare) einen wesentlichen Beitrag leisten.

Die Handvenenerkennung – ergonomisch und hoch sicher

Anwender, die besonders hohe Anforderungen an Hygiene, Sicherheit und Benutzerfreundlichkeit stellen, nutzen die Handvenenerkennung. Da das Handvenenmuster bei jedem Menschen individuell ist, eignet sich dieses biometrische Verfahren besonders

Abb. 3: Biometrische Zutrittssteuerung mittels Handvenenerkennung (Foto: PCS Systemtechnik)

gut zur zweifelsfreien Identifizierung einer Person. Der aktuelle Sensor arbeitet so schnell, dass eine kurze Aufnahme der Handfläche genügt, um einen Datenabgleich mit dem gespeicherten Handmuster-Template durchzuführen.

Auch bei starkem Umgebungslicht und Sonneneinstrahlung arbeitet der Sensor zuverlässig und kann im Außenbereich in wettergeschützter Lage eingesetzt werden. Ein größerer Speicher sorgt dafür, dass Unternehmen die Handvenenerkennung zur Identifikation von bis zu 1.000 Mitarbeitern ohne zusätzliche Karte nutzen können. Die Handvenenerkennung lässt sich auf verschiedene Weise nutzen. Der biometrische Sensor ist zum Beispiel als Einbaumodul erhältlich. Damit lässt er sich in Vereinzelungsanlagen integrieren, aber auch in Aufzüge oder Türkommunikationsanlagen.

Ein wichtiger Pluspunkt ist die Tatsache, dass die Erkennung völlig berührungslos erfolgt. Da das System bei der Erfassung der biometrischen Merkmale nur ein Template speichert, sind keine Rückschlüsse auf eine bestimmte Person möglich. Handvenen-Sensoren bieten in Kombination mit Verschlüsselung des Templates ein hohes Maß an Sicherheit. Einmal installiert, müssen die Sensoren in der Regel nicht mehr gewartet werden. Da die biometrischen Merkmale unter der Hautoberfläche verborgen sind, sind diese vor Außeneinwirkung geschützt und schwer zu fälschen.

Um das gesamte Zutrittssystem zu schützen, ist eine integrierte Firewall erforderlich. Sowohl die Daten der Rechner- als auch die der Leserschnittstellen zu der Zutrittszentrale sollten immer verschlüsselt werden. Für Hochsicherheitsanforderungen sollte eine Zwei-Faktor-Authentifizierung (2FA) genutzt werden. Bei dieser Sicherheitsprozedur muss der Anwender zwei unterschiedliche Merkmale zur Identifikation bereitstellen, z.B. seinen Ausweis plus PIN und/oder ein biometrisches Merkmal wie das Template der Handvenen. Manche Sicherheitsprozesse erfordern mittlerweile eine Mehrfaktor-Authentifizierung, wobei neben den genannten Faktoren, z.B. noch der Ort und oder eine vorgegebene Zeit hinzugefügt werden.

Abb. 4: Zutrittsstelle mit der Möglichkeit der Mehrfach-Authentifizierung mittels PIN, Ausweis/Smartphone und/oder Handvenenerkennung (Foto: PCS Systemtechnik)

DIPL.-ING. WERNER STÖRMER,
Fachautor; Delegierter der PCS im BHE und 2. Vorsitzender im Fachausschuss „Zutritt“