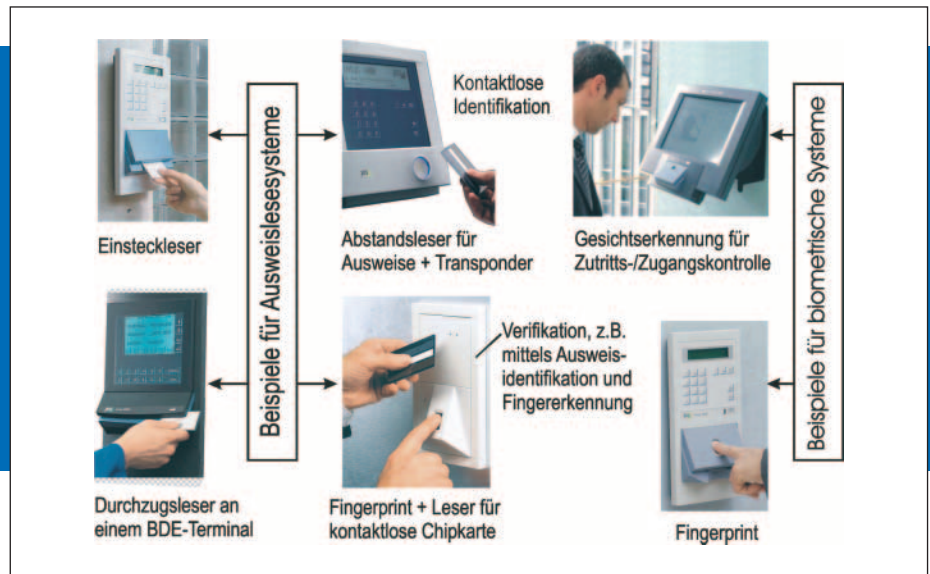


Identifikation und Zutrittskontrolle – Teil II

Zur Prüfung der Zutrittsberechtigung einer Person stehen eine Vielzahl von Identrägertypen und ID-Verfahren zur Verfügung, die sich von der klassischen Ausweis- erfassung bis hin zu biometrischen Erkennungsverfahren erstrecken.



Im ersten Teil von Werner Störmer lasen Sie über verschiedene Verfahren zur Personenerkennung, über Chipkarten als Ausweise und neue Normen. Lesen Sie nun den zweiten und letzten Teil, der sich mit biometrischen Verfahren und mit Empfehlungen zur Systemauswahl auseinandersetzt.

Biometrische ID-Verfahren für Hochsicherheits-Zutrittskontrolle

Hohe Sicherheitsanforderungen verlangen ID-Merkmale, die unverwechselbar mit der Person verbunden sind und eindeutig als personenspezifisch erkannt werden. Die Verfahren zur biometrischen Erkennung sollen die Schwachstellen anderer Identifikationsmethoden ausgleichen oder ergänzen.

Bisher war der Einsatz biometrischer Technologien noch recht kostenintensiv, da die meisten Systeme spezielle Hardware erforderten, um biometrische Muster zu erkennen. Neue Entwicklungen in diesem Bereich haben jedoch die Gerätekosten stark reduziert. So gehören z.B. optische Fingerabdruck-Scanner zum Niedrigpreis-Segment und werden bereits in Zutrittsterminals oder Computertastaturen integriert. Die stark angestiegene Rechenleistung heutiger PCs tut ein übriges, um komplexe Algorithmen zur Extraktion und Erkennung biometrischer Merkmale auch in der praktischen Anwendung nutzbar zu machen.

Je nach Verfahren fallen große Referenzdatenmengen an. Werden diese Daten zentral abgelegt, dann wird bei einer hohen Nutzerzahl nicht nur viel Speicherplatz benötigt, sondern die Suchzeiten für das Auffinden der jeweiligen Referenzdaten verlängern sich (mehrere Sekunden). Durch die Kombination eines biometrischen Ver-

fahrens mit einem Kartensystem lässt sich die Suchzeit verringern, weil nur noch gezielt auf den Datensatz auf der jeweiligen Karte zugegriffen werden muss. Die beiden verbreitetsten Verfahren werden nachfolgend beschrieben:

Fingerprint

Hierbei werden – optisch oder über Sensoren – Grundmuster der Fingerkuppe (Minuzien), deren Tiefe, Breite, Position und Merkmale, als Parameter erfasst und mit einem Referenzmuster verglichen. Das Verfahren zeichnet sich durch die Integrationsfähigkeit des Sensormoduls in Zutrittsgeräten, Tastaturen und PC-Maus sowie eine hohe Benutzerfreundlichkeit aus. Um eine Täuschung des Systems auszuschließen, können ggf. Sensoren zur Lebenderkennung, z.B. zur Bestimmung des Blutsauerstoffgehaltes oder der Pulsfrequenz sowie zur Temperatur- oder Hautwiderstandsmessung, eingesetzt werden.

Das neue Sicherheitsbewusstsein und die mittlerweile attraktiven Preise für den Fingerprint führen verstärkt zum kombinierten Einsatz von Ausweis- mit biometrischen Systemen. Hier wird Sicherheit mit Nutzen in Einklang gebracht. Um ein erfolgreiches Zusammenspiel sicher zu stellen, müssen folgende Grundvoraussetzungen erfüllt sein:

Das biometrische Template wird anstatt in einer Datenbank im relativ sicheren Speicher auf einer kontaktlosen Chipkarte hinterlegt. Die persönlichen biometrischen Daten bleiben in der Verantwortung des Eigentümers.

Dann findet der Abgleich zwischen dem auf der Karte gespeicherten und am Identifikationssystem erfassten Template statt. Bei Übereinstim-

mung erfolgt zur Berechtigungsprüfung die Übertragung der Ausweisnummer an das überlagerte Zutrittskontrollsystem. Nach geprüfter Berechtigung wird z.B. der Zutritt an einer Tür freigegeben.

Die Vorteile dieses Verfahrens liegen nicht nur in der Erhöhung der Systemakzeptanz und Sicherheit, sondern dies erspart auch den Zugriff auf eine Rechner-Datenbank und ermöglicht kurze Erkennungs- und Prüfzeiten.

Gesichtserkennung

Zur Gesichtserkennung wird mittels Kamera automatisch ein Bild 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. Alternativ kann mit Hilfe einer Videokamera die Wärmeabstrahlung der Blutgefäße unter der Gesichtshaut erfasst werden.

Innovative Bildverarbeitungsalgorithmen berechnen aus den digitalisierten Daten der Kameraaufnahme einen Merkmalsdatensatz, der mit dem auf dem Rechner abgelegten und einem einer Person eindeutig zugeordneten Datensatz auf Übereinstimmung geprüft wird. Auch bei unterschiedlicher Mimik oder Position des Gesichts vermag das System aus der Bildverarbeitung die Person sicher zu identifizieren.

Empfehlungen zur Systemauswahl

Die Auswahl des ID-Systems muss nach einer Kosten-/Nutzen-Analyse erfolgen und sich nach



den Anwenderbedürfnissen richten: Bedienerfreundlichkeit, Benutzerakzeptanz, Zuverlässigkeit, Sicherheit und Tauglichkeit unter Berücksichtigung der Umgebungsbedingungen (z.B. bei Außeninstallationen, schmutziger Umgebung, usw.). Abhängig von der Frequentierung je Zutrittsstelle sind insbesondere die Erkennungszeiten zu beachten, hierzu gehört die richtige Positionierung und Handhabung des Identträgers (Ausweis, Transponder oder biometrisches Merkmal) am Identifikationssystem und die Zeit für den Vergleich und die Prüfung der Daten.

Bei der Einführung von Mitarbeiterausweisen ist die uneingeschränkte Nutzungsmöglichkeit zu beachten, damit die Mitarbeiter nicht mit mehreren monofunktionalen Ausweisen, z.B. Zutritts- und Kantinenkarte, hantieren müssen.

Nur der les- und beschreibbare Ausweis mit Chip, unter Umständen auch mit Magnetstreifen, kann multifunktional eingesetzt werden. Die kartengebundene Identifikation ist relativ zuverlässig, sehr preisgünstig und geht meist viel schneller als die Erkennung personenspezifischer Merkmale. Nachteil ist, dass Ausweise verloren oder beschädigt werden können und der Nutzer nicht immer der Besitzer bzw. Berechtigte sein muss.

Dagegen bieten die biometrischen Verfahren eine wesentlich höhere Sicherheit und oft einen größeren Benutzerkomfort, sind jedoch nicht für alle Einsatzarten geeignet. Die Auswahl muss also entsprechend der jeweiligen Anforderungen und Umgebungsbedingungen sorgfältig erwogen werden. Bei den biometrischen Verfahren


fallen sehr große Referenzdatenmengen an, die bei einer hohen Nutzerzahl großen Speicherplatz und relativ lange Suchzeiten benötigen. Auch mit intelligenten Verfahren und schnellen Computern kann der Suchvorgang für die Referenzdaten einige Sekunden dauern. Durch die Kombination mit der Ausweisidentifizierung lässt sich die Suchzeit reduzieren und die persönlichen Referenzdaten bleiben im Eigentum des Besitzers.

Bei den Beschaffungskosten muss zwischen einmaligen Ausgaben beim Kauf des ID-Systems und den laufenden Kosten unterschieden werden. Auch der Aufwand für die Systeminstallation, der Platzbedarf des jeweiligen Systems und die notwendige Wartung, spielt eine wichtige Rolle. Beispielsweise sind Ausweisleser für kontaktlose Chipkarten oder Fingerprintsysteme relativ preiswert, einfach zu installieren und haben den geringsten Platzbedarf. Dagegen arbeitet die Gesichtserkennung meist mit in Standsäulen integrierten Kameras, oft kombiniert mit Spiegel als Positionierungshilfe. Solche Systemeinheiten sind relativ groß, um sie architektonisch einfach und optisch ansprechend integrieren zu können.

Alle aufgeführten Verfahren haben ihre Vor- und Nachteile. Bei der Vielfalt der unterschiedlichen Sicherheitsanforderungen, Einsatzbedingungen und Unternehmenstypen, hat der Anwender somit eine große Auswahlmöglichkeit. Ausführliche Informationen zur Planung, Auswahl und Einführung von Identifikations- und Zutrittskontrollsystemen mit Checklisten zu den einzelnen Themenbereichen enthält das Fachbuch „Arbeitszeitmanagement und Zutrittskontrolle mit System“, das im Luchterhand Verlag, Neuwied (ISBN 3-472-03680-X), erschienen ist.

Werner Störmer

PCS Systemtechnik GmbH • wstoermer@pcs.com

 **Kategorie Zeit + Zutritt**