

Die Guten von den Bösen trennen

Nach dem 11. September sind die Sicherheitsanforderungen gestiegen. Dieser Beitrag erläutert die wesentlichen organisatorischen Maßnahmen zur Einführung einer Zutrittskontrolle und beschreibt die aktuellen Technologien zur Personenidentifikation.

Neue Sicherheitsanforderungen aufgrund von Negativereignissen und Katastrophen sowie Änderungen von Gesetzen und Verordnungen zum Schutz von Mensch und Umwelt sind meist die Gründe für den Start eines Projektes zur Zugangs- und Zutrittskontrolle (ZK). Die Zutrittskontrolle soll das unbefugte Betreten von Gebäuden, Räumen und Arealen verhindern und darin befindliche Werte vor Diebstahl oder Zerstörung schützen.

Moderne ZK-Systeme ermöglichen die einfache Integration in kartengesteuerte Anwendungen, wie die Kantine- (KDE) und Personalzeiterfassung (PZE). Aus Kostengründen ist hier die Nutzung des gleichen Netzwerks, Ausweis- und Identifikationssystems, gegebenenfalls auch des gleichen Terminals, sinnvoll. Bei derart verknüpften

Systemen können mit nur einem Buchungsvorgang der Arbeitsbeginn des Mitarbeiters erfasst und die Zutrittsberechtigung erteilt werden. Ein weiterer Vorteil ist die Nutzung gleicher Stammdaten. Diese beinhalten die Arbeitszeitvereinbarung für den Mitarbeiter, sein Arbeitsprofil sowie seine Buchungs- und Zutrittsberechtigungen, so dass beide Systeme logisch mit den gleichen Basisdaten arbeiten. Eine doppelte zeitintensive Datenpflege entfällt. Häufig wird von Unternehmen oder seinem Betriebsrat trotzdem eine strikte Trennung von ZK und PZE gefordert. Dies ist problemlos möglich. Zumindest sollten aber aus Service- und Kostengründen die gleichen Ausweis- und Lesesysteme eingesetzt werden, wie sie bereits für die PZE üblich sind.

Die ZK ist meist auch Teil eines integralen Sicherheitskonzepts mit Alarmanlagen, Einbruchmeldesystemen und zentraler Leittechnik. Hierzu gehört die Anbindung und Steuerung von Vereinzelungseinrichtungen wie Schranken, Drehkreuze und Türen. Von zunehmender Bedeutung ist auch der Schutz von Programmen und Daten. In der Regel erhalten nur Berechtigte Zugriff auf Rechner und Netzwerk, die sich über ein Passwort oder besser noch Ausweise und/oder biometrische Merkmale am PC-Arbeitsplatz identifizieren können. Die Überprüfung der jeweiligen Zugriffe wird als Zugangskontrolle bezeichnet und sollte nicht mit der Zutrittskontrolle verwechselt werden.

Beispielsweise bei PCs oder Terminals, die zur Verwaltung von Personaldaten

Kompakt

- Die Zutrittskontrolle soll das unbefugte Betreten von Gebäuden, Räumen und Arealen verhindern.
- Die Zutrittskontrolle ist meist auch Teil eines Sicherheitskonzepts mit Alarmanlagen, Einbruchmeldesystemen und zentraler Leittechnik.
- Bei PCs oder Terminals, die zur Verwaltung von Personaldaten oder zur Mitarbeiterselbstbedienung (Employee-Self-Service) eingesetzt werden, sollte eine Zugangskontrolle erfolgen.

oder zur Mitarbeiterselbstbedienung (Employee-Self-Service = ESS) eingesetzt werden, sollte eine Zugangskontrolle erfolgen. Empfehlenswert sind Systeme mit integrierten Identifikationssystemen. Im Beispiel von Abbildung 1 erhält der Benutzer nur Zugriff auf seine Personaldaten am ESS-Terminal, wenn er nach erfolgreicher Ausweisidentifikation – statt Passworтеingabe – sich mittels Fingererkennung eindeutig authentifizieren kann.

Organisatorische Maßnahmen

Im Vergleich zu anderen IT-Vorhaben gelten Zutrittskontrollprojekte als ausgesprochen anspruchsvoll und schwierig. Neben den fachlichen Aspekten muss sich das Projektteam sehr intensiv mit technischen Fragen (Identifikationssysteme, Systemhard- und Software) und mit organisatorischen Regelungen (Betriebs-

vereinbarung, Berechtigungsmodelle) auseinander setzen. Um den gewünschten Nutzen und eine hohe Verfügbarkeit zu erreichen, ist eine sorgfältige Planung, Auswahl, Einführung und ausreichende Systembetreuung sicherzustellen. Wichtig ist zu Beginn des ZK-Projektes die Erarbeitung der Aufgabenstellung, des Umfangs und der Ziele des geplanten Projektes. Seitens des Managements werden vorher meist auch wichtige Restriktionen für die Realisierung definiert wie bestimmte Systemanforderungen, der Kosten- und Zeitrahmen. Weitere Rahmenbedingungen werden durch das vorhandene IT-Umfeld gesetzt.

Von besonderer Bedeutung ist die Prüfung des Sicherheitsbedarfs und der damit verbundenen Festlegung von Sicherheitszonen. Dabei handelt es sich um eine rein organisatorische – auf das jeweilige betriebliche Umfeld bezogene –

Definition. Das Unternehmensgelände und die darin befindlichen Gebäude werden in verschiedene Zonen eingeteilt, für die jeweils individuell der Grad der Sicherheit festgelegt werden kann. Zu unterscheiden sind das betriebliche Anwesen mit Zufahrten, Parkplätze und die verschiedenen Gebäude mit Stockwerken, Abteilungen (vergleiche Abbildung 2). Jede Raum- und Zeitzone kann einer bestimmten Sicherheitsstufe zugeordnet werden.

Mit einer abgestuften Zonensicherung wird zum Beispiel gewährleistet, dass jeder Mitarbeiter den Zutritt zur Kantine erhält aber nur die EDV-Mitarbeiter ins Rechenzentrum dürfen. Um einen Überblick über die Einteilung von Sicherheitszonen innerhalb eines Schutzobjekts zu erhalten, ist es sinnvoll, diese Zonen zum Beispiel mit unterschiedlichen Farben zu kennzeichnen. Dabei

Zutrittskontrolle



Bild 1: Nur der richtige Fingerabdruck gibt den Zugang zum Employee-Self-Service-Terminal frei.

zeichnet werden. Bei sichtbar getragenen Ausweisen lässt sich so mit einem Blick feststellen, ob der Ausweisinhaber Zonenzulassung hat oder nicht. Ergänzend können bereits an Lesegeräten in Zugangsbereichen oder an den Türen Farbmarkierungen angebracht sein. Auch auf Gebäudeplänen sollten die Raumzonen über die Grafiksoftware in verschiedenen Farben darstellbar sein.

Kartengesteuerte oder biometrische Personenidentifikation

wird unterschieden – für Mitarbeiter und Besucher kenntlich gemacht – ob die Zone gesichert und laufend überwacht wird oder für jedermann zugänglich ist. Ausweise können komplett eingefärbt oder auch nur mit einem Farbpunkt gekenn-

Nur Personen, die sich identifizieren können und über eine Berechtigung verfügen, erhalten den Zutritt zum Werksgelände, zu Gebäuden und Sicherheitsbereichen. Da die Identiträger – meist Mitarbeiterausweise – auch für andere kartenge-

steuerte Anwendungen wie Kantinen- und Personalzeiterfassung, genutzt werden, kommt der Auswahl des Identifikationssystems besondere Bedeutung zu. Zur Zutrittskontrolle mit hohen Sicherheitsanforderungen werden verstärkt biometrische Verfahren eingesetzt (vergleiche Abbildung 1, 3 und 4).

Für die klassische Zutrittskontrolle werden heute kontaktlose Chipkarten oder Transponder, zum Beispiel als Schlüsselanhänger eingesetzt. Im Unterschied zu anderen Technologien besitzt die Chipkarte eine integrierte Schaltung zur Informationsspeicherung mit Datenschnittstellen nach außen. Beim Einsatz biometrischer Verfahren, wie Fingerprint oder Gesichtserkennung, können die Referenzdaten in einem entsprechend großen und gegen unerlaubten Zugriff gesicherten Speicher der Chipkarte hinterlegt werden.

Die Chipkartentechnologie ermöglicht auch die Verknüpfung mit anderen Anwendungen. Beispielsweise kann die Geldkarte der deutschen Kreditwirtschaft auch zur Identifikation bei der ZK, PZE und KDE genutzt werden. Auf dem freien Speicherplatz des Kartenchips wird eine Ausweisnummer hinterlegt, mittels der die Überprüfung von Berechtigungen gesteuert werden. Der Vorteil besteht vor allem darin, dass die betreffenden Unternehmen oder Behörden keine Investitionen in die Karten leisten müssen, weil sie bereits bundesweit verbreitet sind. Dabei spricht für die Geldkarte auch, dass das Schlüsselmanagement für gesichertes Auslesen der Daten und damit eine effiziente Kartenechtheitsprüfung bereits auf dem Chip implementiert ist (vergleiche Abbildung 3).

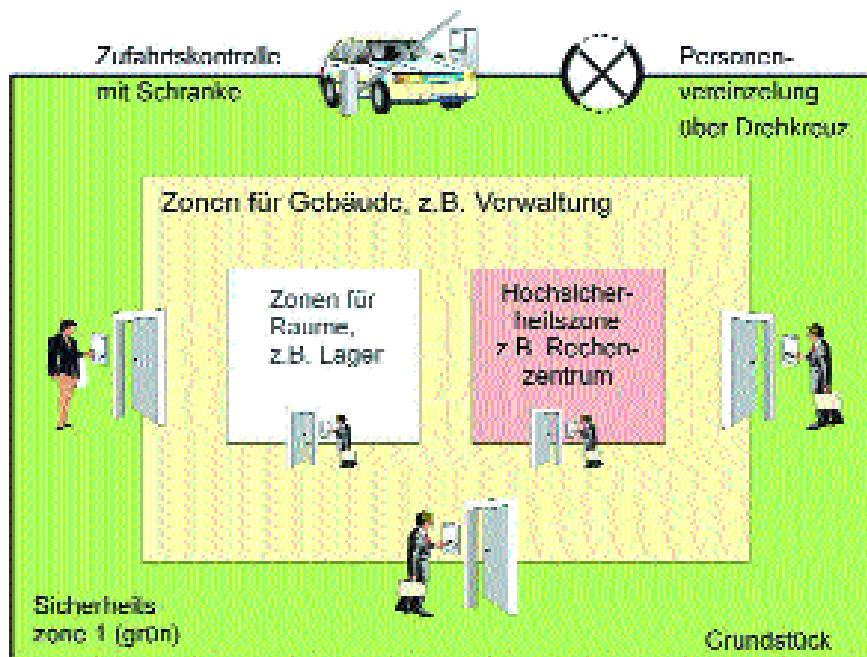


Bild 2: Das Unternehmensgelände und die -gebäude werden in verschiedene Zonen eingeteilt, für die der jeweilige Sicherungsgrad festgelegt wird.

Kontaktlose Chipkarte

Bedingt durch die Art der Datenübertragung und den Aufbau des Lesesystems ist die kontaktbehafte Chipkarte nicht

Mehr zum Thema

Mülder, Wilhelm/Störmer, Werner: Arbeitszeitmanagement & Zutrittskontrolle. Anforderungen, Einführungsstrategien und Beispiele, 3. überarbeitete Auflage, Neuwied 2002, 390 Seiten, 45 Euro

((Cover einfügen))
noch nicht
eingetroffen

für alle Einsatzbedingungen geeignet. Beispielsweise können Fremdkörper oder Feuchtigkeit in die Einstecköffnung des Lesers eindringen. Günstiger ist hier die kontaktlose Chipkarte, bei der die Energieversorgung des Identträgers und der Datenaustausch vom/zum Lesegerät unter Verwendung elektromagnetischer Felder erfolgen. Neben der Karte werden auch so genannte Transponder in diversen Formen und Größen, zum Beispiel als Schlüsselanhänger, angeboten. Abstandsleser werden als integrierte Module für PZE-/ZK-Terminals wie auch als abgesetzte oder eigenständige ZK-Leser angeboten. Hierbei kann die Identifikation im Vorbeigehen erfolgen, unabhängig davon, ob es regnet, schneit oder ob die Karte verschmutzt ist. Dabei hängt die Lesereichweite vom verwendeten System und dessen Empfindlichkeit gegenüber Störungen, aber auch von der

Größe und Art der Antenne im Lesegerät ab.

Während ein herkömmlicher Kartenleser durch Kaugummi, Büroklammern, Papierstückchen oder eingeschüttete Flüssigkeiten einfach außer Funktion gesetzt werden kann, so vermögen es die Abstandsleser, den Ausweis oder Transponder selbst durch Mauerwerk hindurch zu identifizieren; dadurch lässt sich der Leser vandalismusgeschützt installieren.

Dual-Interface- oder Kombikarte

Die Zukunft gehört wohl der Dual-Interface- oder Kombikarte, die sowohl den kontaktlosen als auch den kontaktbehafteten Datenaustausch erlaubt. Dadurch werden die Vorzüge beider Technologien miteinander verbunden: zum einen der Sabotageschutz und die Komfortabilität bei der Identifikation und zum an-

deren die Sicherheit bei Lese-/Schreibvorgängen mit vielen Daten, insbesondere bei Zahlungsfunktionen. Zusätzlich können Dual-Interface-Karten natürlich noch mit Magnetstreifen, Barcodes oder anderen Codierungen versehen werden.

Bei höheren Sicherheitsanforderungen werden biometrische Authentisierungssysteme eingesetzt die Personen anhand physiologischer und verhaltensbedingter Merkmale eindeutig erkennen. Diese biometrischen Merkmale sollen die Schwächen anderer Identifikationsarten wie vergessener PIN oder Ausweis, eliminieren. Bislang waren biometrische Authentisierungssysteme noch relativ teuer, weshalb sie hauptsächlich für polizeiliche oder militärische Sicherheitsanwendungen genutzt wurden.

Mittlerweile wurde die Technik – und damit auch die Akzeptanz dieser Systeme



Bild 3: Das Terminal kombiniert die Kontrolle per Fingerabdruck mit einem Chipkartenleser für die Geldkarte.

me – soweit verbessert, dass der Einsatz für eine sichere und zuverlässige Erkennung genutzt werden kann. Um die Identität einer Person authentifizieren zu können, werden die biometrischen Merkmale als Referenzdaten in Datenbanken gespeichert und zur Berechtigungsprüfung aufgerufen. Empfehlenswert ist die Speicherung der umfangreichen Referenzdaten mittels Datenkompression auf einer kontaktlosen Chipkarte. Bei der Ausweisidentifizierung entfällt die Suchzeit in der Datenbank. Mittlerweile werden folgende Verfahren eingesetzt:

- Verfahren, die statische physiologische Attribute (zum Beispiel Fingerabdrücke, Handgeometrie, Netzhautmuster) erfassen.
- Verfahren, die variable und dynamisch-physiologische Attribute (zum Beispiel Gesicht, Stimme) oder verhaltensabhängige Merkmale wie

Schreibrhythmus auf einer Computertastatur oder eine Unterschrift per Hand zur Überprüfung heranziehen.

- Multimodale Verfahren, die mehrere Merkmale, sowohl statische als auch dynamische, kombiniert erfassen, um eine höhere Erkennungsgenauigkeit zu erreichen. Die drei wichtigsten biometrischen Authentifizierungssysteme werden nachfolgend kurz erläutert:

Schnelle Identifikation per Fingerabdruck

Die neuartigen Module zur Fingererkennung sind so entwickelt, dass diese anstelle von schmutzanfälligen optischen Scannern, mit Silizium-Chips oder CCD-Sensormodulen arbeiten. Diese winzigen Module registrieren die Mikrostruktur der Haut und ermöglichen zum Beispiel die Integration in ZK- und ESS-Terminals. Der aufgelegte Finger ersetzt oder ergänzt



Bild 4: Auch die Unausgeschlafenen werden reingelassen, weil die Software mithilfe einer Kamera unterschiedliche Mimiken eines Gesichts erkennt.

also die Ausweis- und/oder PIN-Eingabe. Gegen Ungenauigkeiten durch Narben, Schmutzpartikel oder Finger-Verletzungen werden Fehlerkorrektur-Algorithmen eingesetzt. Um eine Täuschung des Systems auszuschließen, können gegebenenfalls Sensoren zur Lebenderkennung, zum Beispiel zur Bestimmung des Blutsauerstoffgehaltes oder der Pulsfrequenz sowie zur Temperatur- oder Hautwiderstandsmessung, eingesetzt werden.

Langsame Gesicht- und Spracherkennung

Zur Gesichtserkennung wird am Kontrollpunkt mittels Kamera automatisch ein Bild der zu identifizierenden Person aufgenommen (vergleiche Abbildung 4). Innovative Bildverarbeitungs-Algorithmen berechnen aus den digitalisierten Daten der Kameraaufnahme einen Merkmalsdatensatz, der mit dem Rechner abge-

legt und der Person eindeutig zugeordneten Datensatz auf Übereinstimmung geprüft wird. Auch bei unterschiedlicher Mimik des Gesichts vermag das System, aus der Bildverarbeitung die Person sicher zu identifizieren. Beim Spracherkennungssystem werden verschiedene Merkmale der Stimme des Betreibers abgespeichert. Im Überwachungsmodus wird gewährleistet, dass nur Personen einen Zutritt erhalten, deren Sprache, nach Nennung ihres Passwortes, wiedererkannt wird. Zur Erhöhung der Erkennungssicherheit kann zusätzlich eine Analyse der Lippenbewegung bei der Spracheingabe erfolgen. Für die Bewegungsanalyse extrahiert das Verfahren einzelne Bilder aus einer Videosequenz. Mit der Berechnung optischer Flussvektoren entsteht ein charakteristisches biometrisches Muster. Um die Sicherheit noch mehr

Zutrittskontrolle

zu erhöhen, können auch verschiedene biometrische Merkmale wie Gesicht, Sprache und Mimik, kombiniert überprüft werden. Solche Systeme können auch so programmiert werden, dass bei Ausfall einer Erkennungsart (zum Beispiel durch laute Geräusche oder grelles Licht) zwei eindeutig erkannte Merkmale ausreichen.

Die Auswahl des Identifikationssystems ist abhängig von der erforderlichen Sicherheit. Bei der Auswahl sind vorrangig die Akzeptanz bei der Belegschaft und die Frequentierung (zum Beispiel pro Zutrittsstelle) zu beachten. Die kartengebundene Identifikation geht meist sehr viel schneller als die Erkennung personenspezifischer Merkmale. Dagegen bieten die biometrischen Verfahren eine wesentlich höhere Sicherheit, sind jedoch nicht für alle Einsatzarten geeignet. Die Auswahl muss also entsprechend der jeweiligen Anforderungen und Umgebungsbedingungen sorgfältig erwo-gen werden.

Unterschiedliche Systemtypen und Funktionen

Abhängig von der Unternehmensgröße und der benötigten Sicherheit werden Lösungen mit autonomen Zutrittsgeräten oder Systeme mit vernetzten ZK-Terminals angeboten. Soweit nur eine oder wenige Zutrittsstellen für eine geringe Mitarbeiteranzahl gesichert werden müssen, kann eine Standalone-Lösung eingesetzt werden. Bei der autonomen ZK arbeiten die Terminals eigenständig und ohne Verbindung zu einem Rechner. Die Gerätesoftware hat primär die Aufgabe, eine Berechtigungsprüfung für den Zutritt, zum Beispiel anhand der Ausweis- und/oder PIN-Eingabe vorzunehmen. Das ZK-Terminal steuert die Zutrittsberechtigungen über gespeicherte Tabellen, in denen die Zeitprofile für Personengruppen oder einzelne Mitarbeiter hinterlegt werden.

Komfortabler sind vernetzte Systeme mit Funktionen einer übergeordneten ZK-Zentrale, an der abgesetzte ZK-Leser

oder Terminals angeschlossen werden. Diese Systeme bieten umfangreiche Software und Stammdatenverwaltung an. Dabei ist die mögliche Anzahl und Art der Vernetzbarkeit, der anzuschließenden ZK-Geräte zu beachten. Durch Aufteilung bestimmter Softwarefunktionen und Prüfungen im Rechner oder im Terminal (aus Sicherheitsgründen) können Zeitoptimierungen erreicht werden. Außerdem können die Mitarbeiter Terminals an verschiedenen Ein-/Ausgängen benutzen. Auf die im ZK-Server gespeicherten Daten kann von verschiedenen Stellen (zum Beispiel Pförtner) und Abteilungen zugegriffen werden.

Je nach Sicherheitsgrad werden in der Software unterschiedliche Funktionen unterstützt. Am einfachsten sind Türöffnungssysteme, bei der jeder Firmenangehörige, der eine freigegebene Karte hat, zu jeder Zeit die Türen öffnen kann. Die weiter gehende Zutrittskontrolle arbeitet zusätzlich mit einer Zeit- und Raum-zonensteuerung. Erst nach erfolgreicher Prüfung der zeitlichen und örtlichen Zutrittsparameter wird die Tür geöffnet. Die Öffnungszeiten werden über die Tabellen im System verwaltet und über ein entsprechendes Programm in die entsprechenden Terminals verteilt.

Protokolle zeichnen die Bewegungen auf

Ein zusätzliches Modul der ZK-Software ist die Speicher- und Protokollierungsfunktion. Es wird gespeichert welcher Mitarbeiter, zu welcher Zeit, an welchem Ort (zum Beispiel Tür, ZK-Gerät) eine zulässige oder unberechtigte Zutrittsbuchung vorgenommen hat. Der Vorteil dieses Verfahrens besteht darin, dass jederzeit festgestellt werden kann, welche Personen sich im Moment in welchen Räumen/Sicherheitszonen des Unternehmens aufhalten.

Bei Systemen mit Alarmfunktion wird ereignisabhängig, zum Beispiel unzulässiger Zutrittsversuch oder Ausfall von ZK-Einrichtungen, ein Alarm ausgelöst. Die jeweiligen Reaktionen werden über

entsprechende Konfigurationstools definiert. Dabei sind auch technische Probleme (zum Beispiel defekter Leser) oder Bedienfehler zu berücksichtigen. Alarme können direkt an eine Zentrale zur Bearbeitung weitergeleitet oder lediglich protokolliert und archiviert werden. Letzteres empfiehlt sich bei unberechtigten Zutrittsversuchen, weil es ja bei dem Versuch bleibt und die Person über die Buchung identifizierbar ist.

Ab drei Personen ist Schluss

Überwachungssysteme kontrollieren das Verlassen (nach berechtigtem Zutritt) von Räumen, die vorhandene oder zulässige Zahl von Personen pro Raum, den Raumwechsel (Person B darf nicht von Raum Y nach Raum Z) oder die Zutritts-wiederholungsperre. In allen Fällen sind die organisatorischen Maßnahmen zu beachten, zum Beispiel wenn sich nicht mehr als drei Personen gleichzeitig in einem Raum aufhalten sollen und eine vierte Person Einlass verlangt: Soweit die Anwesenden aufgefordert werden sollen, den Raum zu verlassen, ist eine optische oder akustische Signalgebung erforderlich. Auch für den Einlassbegehrenden muss eine Anzeige erfolgen, warum er nicht eintreten darf. Hierfür könnte der Einsatz eines ZK-Terminals mit mehrzeiligem Display, auf dem eine entsprechende Bedienungsführung angezeigt wird, sinnvoll sein.



Autor

Werner Störmer,
Prokurist und
Vertriebsleiter, PCS
Systemtechnik GmbH,
wstoermer@pcs.com

