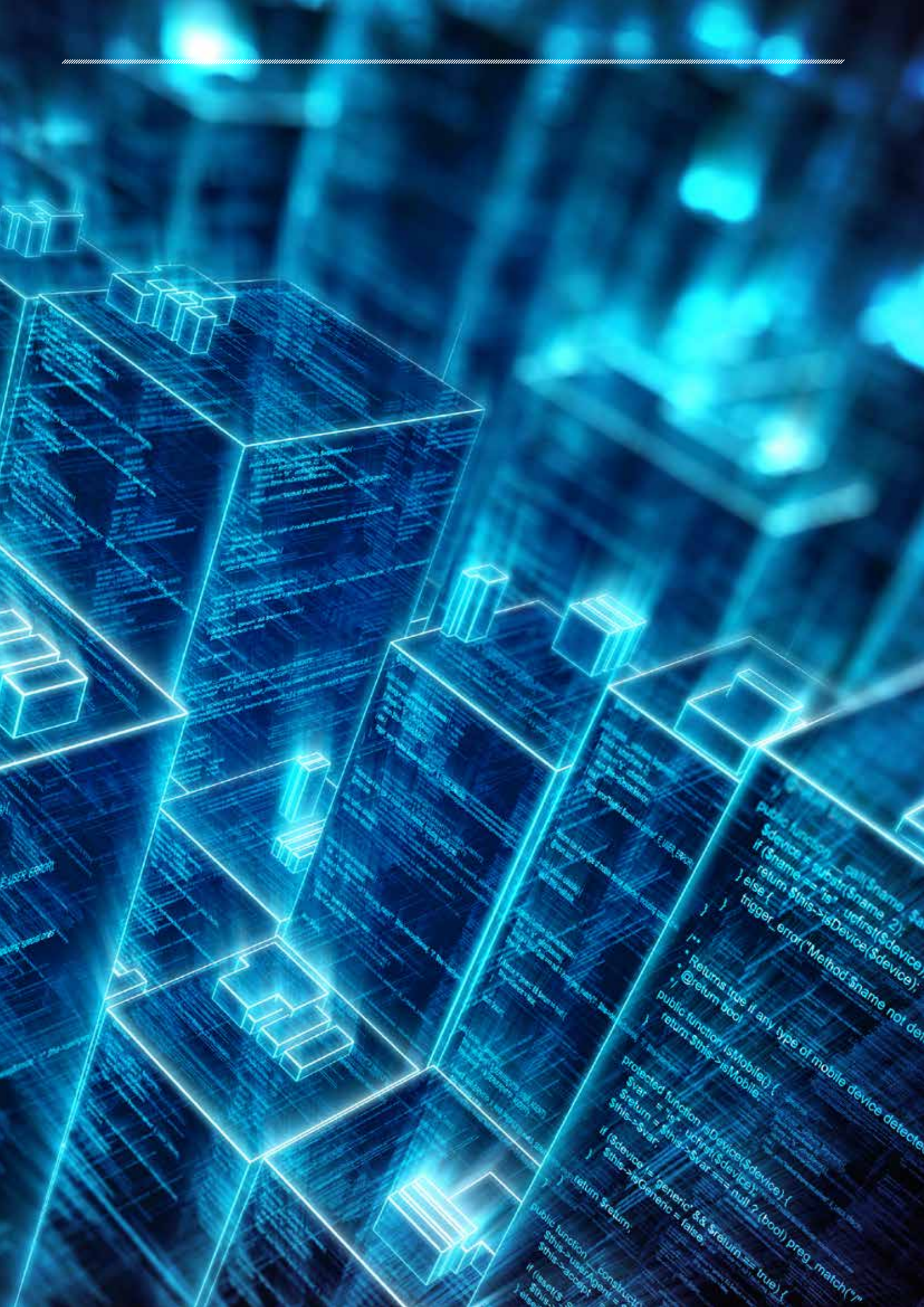
SES
Verband Schweizerischer Errichter von Sicherheitsanlagen

//BUSINESS-DOSSIER//

Evaluation eines Zutrittskontroll-systems



INHALTSVERZEICHNIS

Impressum

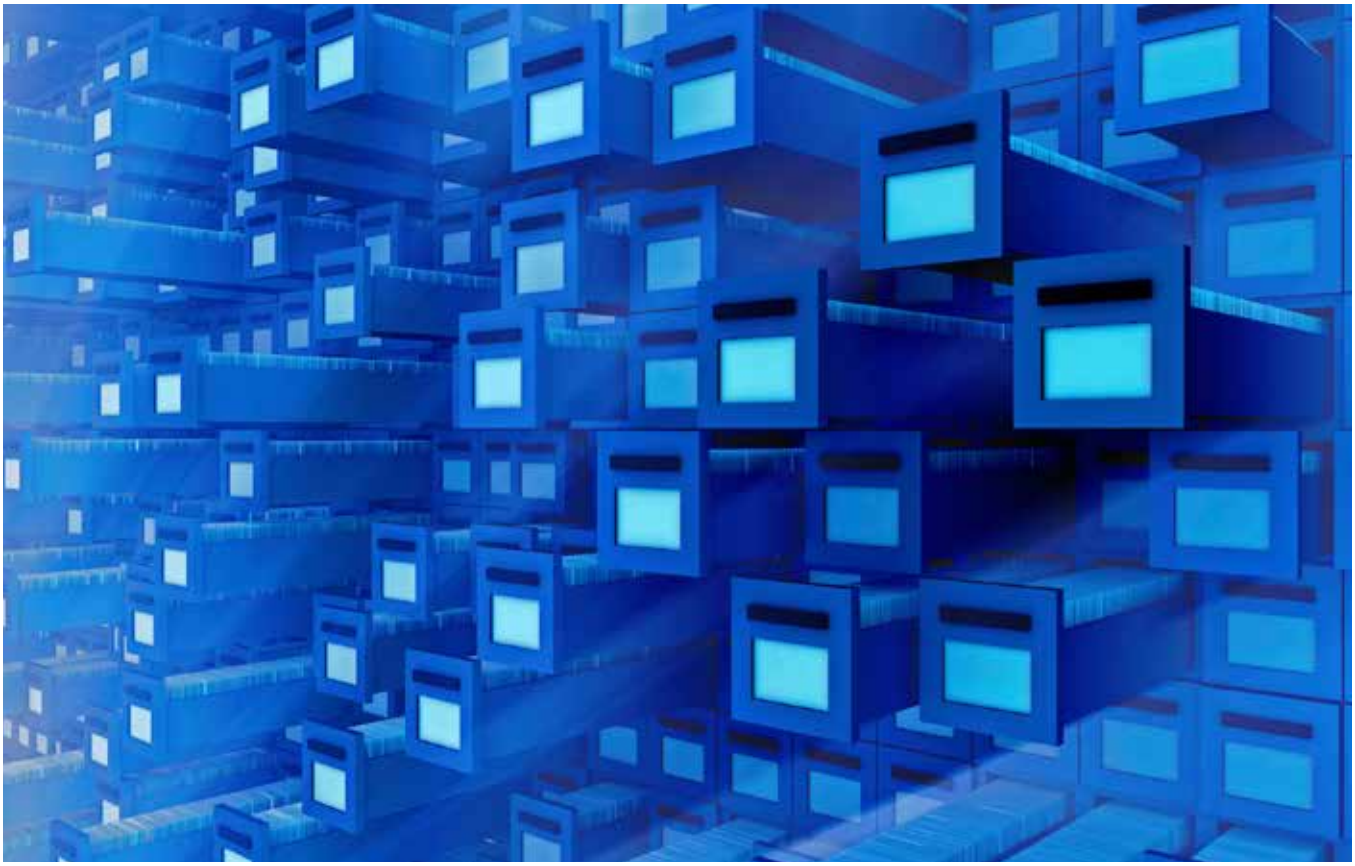
Herausgeber	Verband Schweizerischer Errichter von Sicherheitsanlagen SES, 3052 Zollikofen
	Sektion Sicherheit Untergruppe Access Control (AC) | www.sicher-ses.ch
Quelle	Markus Graf | Siemens Schweiz AG | Fachlehrer Lehrgang Projektleiter Sicherheit
Redaktion	Andreas Stettler, ask andreas stettler kommunikation, Hauptgasse 33, 4600 Olten | www.ask-olten.ch
Gestaltung	mosaiq – integrierte kommunikation, Hauptgasse 33, 4600 Olten | www.mosaiq.ch
Druck	Impress Spiegel AG, media + print, Bühlstrasse 49, 4622 Egerkingen | www.impress.ch

/// Eine Einführung für «professionelle Laien»

Es ist nicht einfach, den Überblick über das umfangreiche Angebot an Zutrittskontrollsystemen zu behalten. Gerade weil so vieles zu beachten ist, kann ebenso vieles falsch gemacht werden. Ob ein neues Zutrittssystem angeschafft oder das bisherige lediglich erweitert oder erneuert werden soll, hängt von zahlreichen Faktoren ab. Der wichtigste ist, dass man nicht nur die Aufgaben der Zutrittskontrolle im Allgemeinen und die vielseitigen Anforderungen an ein solches System kennt, sondern für seinen individuellen Anwendungsfall genau definiert.

Dieses vergleichsweise kompakte Werk ist für jene gedacht, die sich zwar mit dem Thema Zutrittskontrolle befassen und die Beschaffung oder Erweiterung eines solchen Systems vorbereiten, aber keine entsprechenden technischen und branchenspezifischen Kenntnisse mitbringen. Wir haben uns bemüht, in verständlicher Sprache und ohne allzu buntes Feuerwerk von Fachausdrücken und technischen Beschrieben eine Einführung in diese komplexe Welt zu geben, und deshalb bewusst eine teilweise Unvollständigkeit in Kauf genommen.

Das vorliegende Dossier basiert auf den viel detaillierteren Schulungsunterlagen des Verbandes Schweizerischer Errichter von Sicherheitsanlagen SES für angehende «Projektleiter Sicherheit». Die SES-Untergruppe Access Control (AC) und die SES-Fachkommission Ausbildung verantworten den fachlichen Inhalt und die Durchführung des Lehrgangs, in Zusammenarbeit mit der Zürcher Fachhochschule in Winterthur.



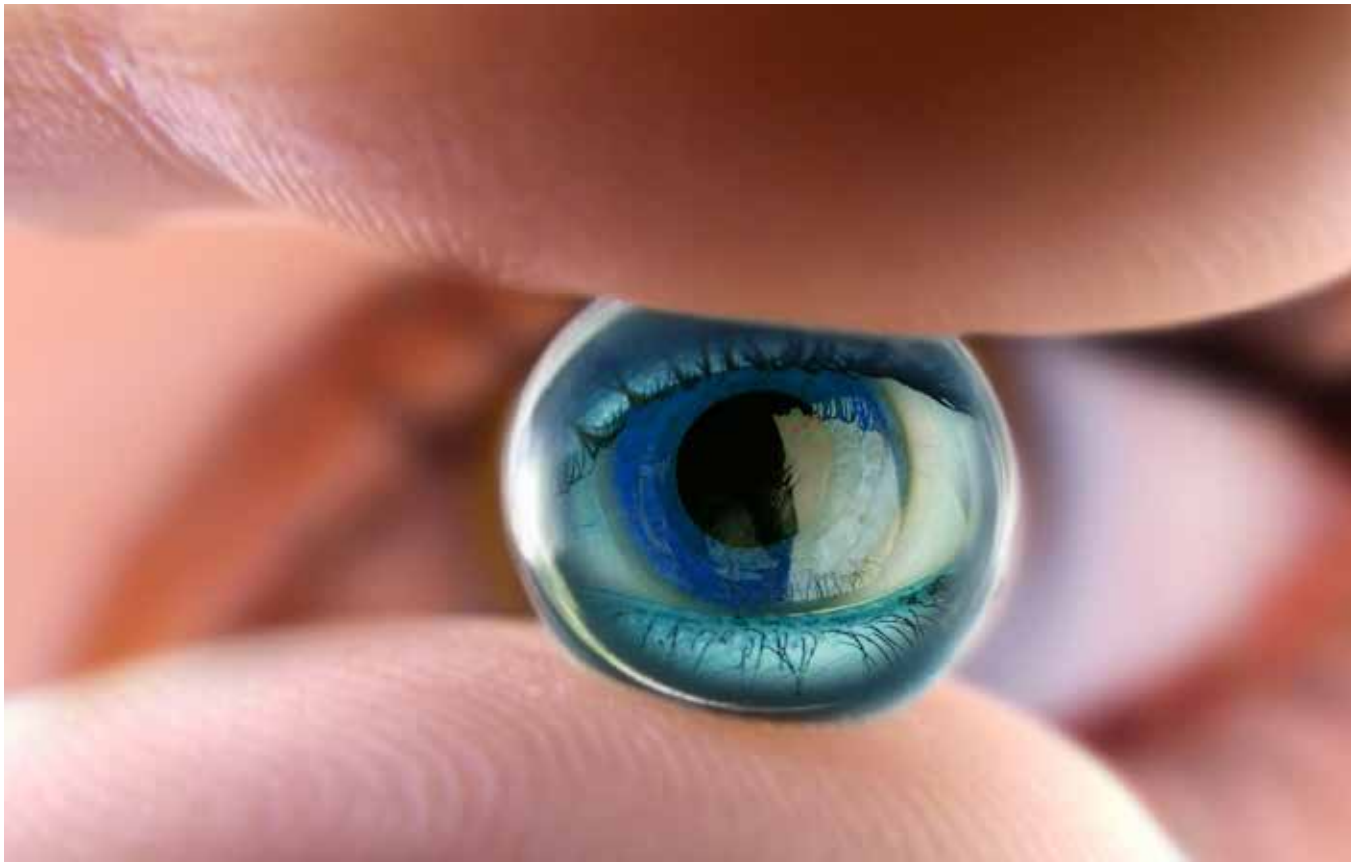
SCHUTZ VON EINRICHTUNGEN UND GEISTIGEM EIGENTUM

Bei der Evaluation eines Zutrittssystems ist es wichtig, die Entwicklung und Aufgabe der Zutrittskontrolle und die vielseitigen Anforderungen an ein Zutrittskontrollsystem zu kennen.

Von einem namentlich nicht bekannten Mann stammt diese Maxime der Zutrittskontrolle: **Berechtigte beim Zutritt nicht behindern und Unberechtigte den Zutritt verwehren.**

Zutrittssysteme sind heute auf einem technologisch sehr fortschrittlichen Stand und verwenden Komponenten, die futuristisch anmuten. Doch je mehr Hightech, umso wichtiger die Frage nach Sinn und Unsinn der einsetzbaren Technologien. Eine frühzeitig durchgeführte, gründliche Evaluation gibt Auskunft darüber, welches System die gestellten Aufgaben am besten bewältigt. Immer vorausgesetzt, dass es die gesetzlichen Normen erfüllt und der Umgang mit den aus der Zutrittskontrolle gewonnenen Daten wohl überlegt ist.

Sind die Rahmenbedingungen einmal geklärt, sind weitere Fragen zu beantworten. Welche Systeme lässt die Architektur überhaupt zu? Was wollen die einzelnen Anwender? Sollen die Systeme miteinander vernetzt werden? Einmal installiert, ist das Projekt längst nicht abgeschlossen. Ein Zutrittssystem geht einher mit der lebenslänglichen Verpflichtung, das System technisch zu warten und funktionsfähig zu halten. Service und Unterhalt spielen eine nicht zu unterschätzende Rolle.



/// Aufgaben der Zutrittskontrolle

WER, WANN, WO?

Die Zutrittskontrolle (ZuKo) regelt den Zutritt zu Gebäuden oder schützenswerten Bereichen nach den Vorgaben «Wer, wann, wo?» und allenfalls «mit wem?» Die Berechtigungen können einmalig, zeitlich begrenzt oder unbegrenzt sein. Die Überprüfung der Rechte kann durch eine Person, ein System oder in Kombination der beiden erfolgen.

Ein Zutrittskontrollsystem ist ein elektronisches Mittel zur Durchsetzung der Zutrittskontrolle und prüft automatisch die Berechtigung einer Person, ein bestimmtes Gebäude, einen Bereich oder Raum betreten zu dürfen, erhöht die Sicherheit und unterstützt die betrieblichen Abläufe.

Ein Zutrittskontrollsystem organisiert den Zutritt über ein vom Betreiber festgelegtes Regelwerk. Berechtigungen werden nach personenbezogenen, räumlichen und zeitlichen Kriterien zugewiesen. Somit wird nur Personen Zutritt gewährt, die sich beispielsweise mit Karte, Ausweis, PIN-Code oder biometrischen Merkmalen zu erkennen gegeben haben.

Die heutige Zutrittskontrolle basiert auf baulichen, organisatorischen und elektrotechnischen Massnahmen. Damit schützen wir Organisationen, Gebäude, Einrichtungen und vor allem Menschen vor Übergriffen und Bedrohungen durch Unbefugte und verhindern den Diebstahl von geistigem Eigentum. Übergriffe in Unternehmen geschehen oft aus Unachtsamkeit, zufällig-situativ oder im Rahmen geplanter krimineller Machenschaften. Übrigens: ca. 70 % der Computerkriminalität wird von eigenen Mitarbeitern begangen.

Die besondere Herausforderung bei der Zutrittskontrolle ist, Berechtigte so wenig wie möglich in ihrer Bewegungsfreiheit einzuschränken, Unberechtigten aber den Zutritt lückenlos zu verwehren. Somit hat die ZuKo auch eine wichtige präventive Aufgabe, indem sie potentielle Täter abschreckt. Sie verhindert zwar keine Übergriffe von Berechtigten, ermöglicht aber deren Identifizierung im Ereignisfall.

/// Entwicklung der Zutrittskontrolle

VON DER ZIEHBRÜCKE ZUR ELEKTRONISCHEN ZUTRITTSKONTROLLE

Das Bedürfnis nach Sicherheit ist so alt wie die Menschheit, und damit verbunden das Bedürfnis nach Zutrittskontrolle. Zu wissen, dass sich nur berechtigte Personen in einem bestimmten Bereich aufhalten, gibt den Menschen Sicherheit. Was im Mittelalter noch mit befestigten Städten und Wachposten an den Stadttoren gelöst wurde, konnte später dank der Entwicklung der Mechanik und Erfindung des Schlosses vereinfacht werden.

Mit der mechanischen Schliessanlage hielt der Zylinder Einzug in die Zutrittskontrolle. Die Prüfung der Zutrittsrechte erfolgte nicht mehr im Schloss, sondern im mechanischen Zylinder. Er liess sich nicht nur in verschiedene Schlösser einbauen, sondern erlaubte erstmals die Vergabe von statischen Zutrittsrechten, indem jeder Schlüssel sein eigenes Bohrmuldenmuster aufwies. Auch eine Schliessanlagenplanung wurde möglich.

Der Verlust eines Schlüssels hat meist hohe Kosten zur Folge: Je nach Konzept müssen mehrere oder alle Zylinder ausgewechselt werden. Die geringen Beschaffungskosten können über den möglicherweise teuren Betrieb hinweg täuschen.

Mit statischen Zutrittsrechten kann das «Wer» und «Wo», aber nicht das «Wann» geprüft werden. Das änderte sich mit der Elektrotechnik, die regelrechte Quantensprünge in der Weiterentwicklung und Perfektionierung von Zutrittssystemen auslöste. Schlüssel und Zylinder werden mit elektronischen Komponenten ausgerüstet, Rechte werden mechanisch und/oder digital geprüft und mit Zeitprofilen erweitert. Verlorene Schlüssel können gesperrt werden, ein Ersatz der Zylinder ist nicht notwendig.

Anstelle von Zylindern und Schlüsseln wurden jetzt Zutrittskontrollleser und Karten mit Magnetsteifen eingesetzt. Die ersten Produkte erlaubten allerdings noch keine Vernetzung, und Konfigurationsänderungen brauchten viel Zeit, weil sie vor Ort, d.h. an jeder Türe vorgenommen werden mussten. Erst die Vernetzung der Komponenten und die zentrale Verwaltung der Zutrittsrechte mit einer Software erlaubte Änderungen zeitgerecht vorzunehmen, reduzierte den administrativen Aufwand und ermöglichte eine zentrale Protokollierung der Bewegungen (wer, wann, wo).

In den 1970er-Jahren wurden die ersten Karten mit Magnetstreifen eingesetzt. Sie boten jedoch wenig Sicherheit, weil die Daten einfach kopiert und ausgelesen werden konnten. Obwohl kostengünstig, waren diese Systeme anfällig auf Verschleiss, die Leseköpfe verschmutzten, die Magnetstreifen auf den Karten nutzten sich schnell ab, zerkratzten oder verloren ihre Codierung. Der Magnetstreifen wurde bald von neuen Technologien abgelöst: In die Karten eingelegte Kupfer- und Codefolien, die induktiv oder via Infrarot ausgelesen wurden.

In den 80er-Jahren kamen die ersten kontaktlosen Lesesysteme auf den Markt. Der Radio Frequency Identification Device (RFID) erlaubt es, Informationen wie z.B. die Kartennummer über eine Lesedistanz von mehreren Zentimetern zu übertragen. Die Leistungssteigerung in der Elektronik ermöglichte in den letzten Jahren immer sicherere und multifunktionalere Lösungen.

Und was bringt die Zukunft?

Die RFID-Technologie wird auch in den kommenden Jahren Kernelement der Zutrittskontrolle bleiben, deren Verschlüsselung jedoch ausgeklügelter und somit sicherer wird. Die Lebensdauer der Technologien wird immer kürzer, weshalb es umso wichtiger ist, dass die Firmware der eingesetzten Komponenten nachgerüstet werden kann.

Auf den RFID-Standards aufbauend, wird die Near Field Communication (NFC) mittels Mobiltelefonen auch in der Zutrittskontrolle eine Rolle spielen. Anders als bei RFID, wo eine Komponente entweder Transponder oder Leser ist, können NFC-Geräte beides sein. Moderne Handys sind bereits mit dieser Technologie ausgerüstet und können als Identifikationsmedium verwendet werden. Zutrittsrechte werden ortsunabhängig über das Telefonnetz übermittelt (ein Vorteil gegenüber Chipkarten) und stehen dem Anwender ohne aufwändige Infrastruktur sofort zur Verfügung. NFC-Anwendungen eignen sich vor allem bei räumlich weit verteilten Objekten. Die Lesedistanz zwischen Mobiltelefon und Zutrittsleser bleibt allerdings, wie bei RFID, auf wenige Zentimeter beschränkt.

Biometrische Verfahren (Messen und Auswerten von personenspezifischen Merkmalen) können anstelle oder in Ergänzung zu RFID verwendet werden. Diese Technologie ist zwar in aller Munde, in der Praxis jedoch noch weniger verbreitet als allgemein angenommen wird. Noch sind die breitere Akzeptanz in der Bevölkerung wie auch griffigere Gesetze notwendig.

Bei Grossinstallationen zeichnet sich ein Trend zu sogenannten Meta-Managementsystemen ab. Dabei werden mehrere bestehende Zutrittskontrollsysteme auf einer übergeordneten Plattform miteinander verknüpft. Ebenfalls absehbar ist die Verschmelzung der ZuKo mit der Gebäudetechnik. Mit der vereinfachten Vernetzung via Bussysteme können somit Licht, Klima, Beschattung, Zutritt und weitere Elemente zentral gesteuert werden.

SAS, Software as a Service sowie Cloud-Lösungen werden auch bei Zutrittssystemen Einzug halten.

DAS SCHWÄCHSTE GLIED IN DER KETTE IST DER MENSCH

Jedes Zutrittskontrollsystem besteht im Wesentlichen immer aus denselben Grundelementen.

Mensch und Organisation

Der Mensch wird absichtlich als Systemkomponente genannt, weil er meist das schwächste Glied in der Kette ist. Denn das Schutzziel kann nur dann erreicht werden, wenn sich alle betroffenen Personen den angeordneten Massnahmen unterziehen. Vor der Installation eines Zutrittskontrollsystems sollen deshalb die Benutzer über dessen Sinn und Zweck informiert und dazu motiviert werden, es ordnungsgemäss zu benutzen. Je komfortabler die Bedienung des Systems, umso höher dessen Akzeptanz. Das gleiche gilt für jede Zusatzmassnahme (z.B. PIN-Code, biometrische Kontrolle): sie muss für die geforderten Schutzziele unumgänglich und für die Benutzer nachvollziehbar sein.

Ausweis

Der Ausweis dient als Identifikationsmittel für das System. Es wird vorausgesetzt, dass er vom rechtmässigen Besitzer benützt wird. Wir sprechen also von einer Ausweis- und nicht von einer Personenidentifikation.

Leser

Der Leser dient zum Erfassen der Ausweisinformation und zur Übermittlung derselben an die Auswertungseinheit. Je nach System ist diese im selben Gehäuse wie der Leser oder in einem separaten Gehäuse (z.B. einem Türkontroller) eingebaut.

Zutrittskontroll-Zentrale

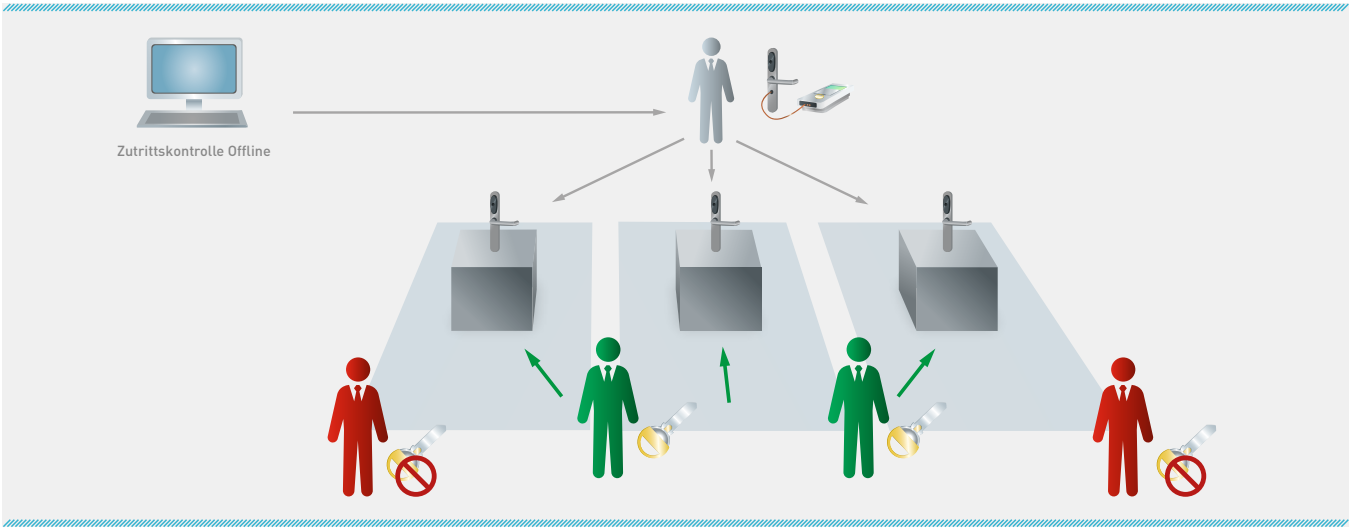
Die Zutrittskontrollzentrale (ZKZ), auch als Kontroller und Datenkonzentrator bezeichnet, prüft ein Zutrittsbegehren und erteilt oder verweigert die Türfreigabe. Dieser Vorgang ist auch ohne permanente Verbindung zum Server möglich, weil die benötigten Daten (z.B. Identifikationsmerkmal der Karte, Berechtigungen) in einer lokalen Datenbank gespeichert werden. Die Zentrale sammelt zudem Ereignisdaten und übermittelt sie für die lückenlose Protokollierung und Analyse an den Server. Je nach System können auch mehrere ZKZ untereinander kommunizieren, um sich gegenseitig «auf dem neusten Stand zu halten».

Türausrüstung

Als Gegenstück zum Zutrittsleser setzt der sogenannte Aktor elektronische Befehle in mechanische Bewegung um und gibt nach positiver Prüfung in der Zentrale den Zutritt an der Türe frei. Abhängig von den Anforderungen an die mechanische Sicherheit, den Brandschutzvorschriften sowie der Flucht- und Rettungswegtechnik, werden Motor- und Elektroschlösser wie auch Elektrotüröffner als Aktoren eingesetzt.

Strom- und Notstromversorgung

Ein Zutrittskontrollsystem muss eine maximale Verfügbarkeit aufweisen. In den meisten Fällen werden die Zentrale sowie die eigenen Peripheriegeräte (Leser, Türsteuermodul usw.) mit einer eigenen (Not-) Stromversorgungen gespeist. Die bauseitigen Türeinrichtungen wie Motor- und Elektroschlösser, Elektrotüröffner oder gar elektrische Antriebe werden vielfach mit einer eigenen dezentralen Speisung versorgt. Es empfiehlt sich, bei der Abnahme auch den Notstrombetrieb zu testen!



Offline-Zutrittskontrolle mit digitalen Türkomponenten: «Grau» lädt die Berechtigungen auf die Türkomponenten; «Grün» hat eine entsprechende Berechtigung auf seinem Medium, «Rot» nicht.

OFFLINE ODER ONLINE?

Es gibt verschiedene Systemkonzepte, die sich je nach Hersteller unterscheiden. Bei den elektronischen Zutrittskontrollsystemen wird zwischen Online- und Offline-Lösungen unterschieden. Bei den Offline-Lösungen können die Zutrittsrechte auf die digitalen Türkomponenten oder auf die Identifikationsmedien (Ausweis, Anhänger, Schlüssel) geschrieben werden.

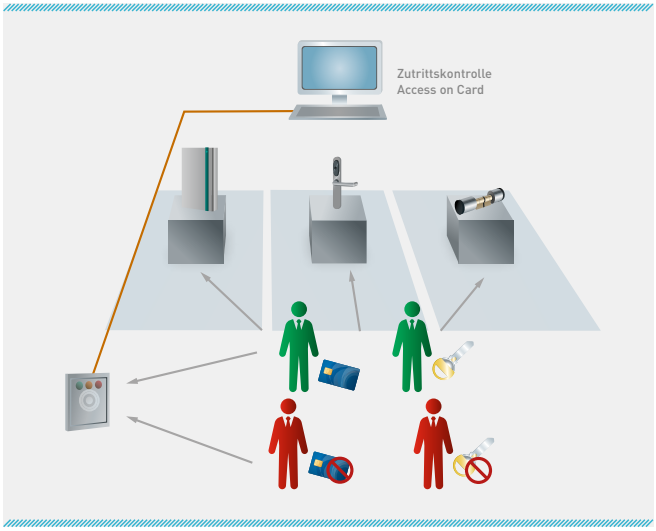
Offline-Zutrittskontrolle 1: Zutrittsrechte in den digitalen Türkomponenten

Offline-Systeme bestehen aus digitalen Zylindern, Beschlägen und Zutrittslesern. Einige Anbieter arbeiten auch mit digitalen Schliesszylindern, die mit einem Schlüssel mit Chip geöffnet werden können.

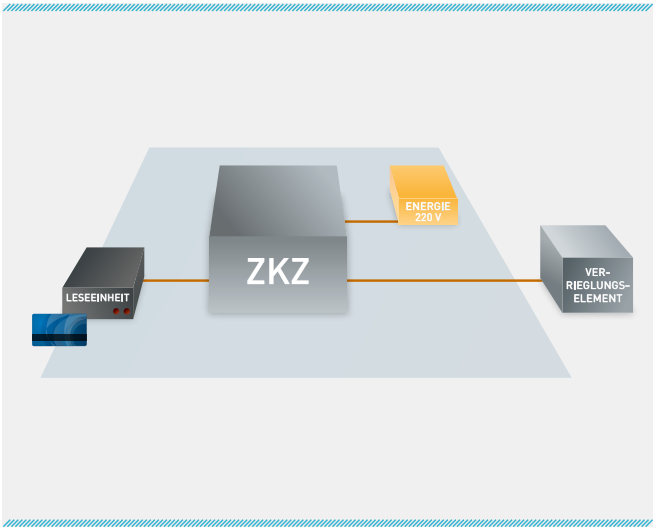
Die Zutrittsrechte und Zeitprofile werden mit einer Software zentral verwaltet und mit einem Programmer auf die digitalen Türkomponenten geladen. Nach jeder Änderung oder Löschung ist diese lokale Programmierung notwendig.

Vor- und Nachteile

- ⊕ Keine Verkabelung notwendig
- ⊕ Geringer Montage- und Installationsaufwand
- ⊕ Einfaches Nachrüsten von Türen
- ⊖ Zutrittsrechte müssen lokal auf die Türkomponenten geladen werden
- ⊖ Zutrittsrechte sind nicht sofort verfügbar
- ⊖ Kartensperrungen sind nicht sofort wirksam



Offline-Zutrittskontrolle mit Zutrittsrechten auf dem Medium: «Grün» hat seine Berechtigungen am Update-Leser auf sein Medium geladen und aktualisiert, «Rot» nicht.



Autonome Zutrittskontrolle

Offline-Zutrittskontrolle 2: Zutrittsrechte auf dem ID-Medium

Die Zutrittsrechte und Zeitprofile werden mit einer Software zentral verwaltet und mittels Update-Leser auf die ID-Medien (Ausweise, Anhänger etc.) geschrieben. Die Zutrittsrechte können verändert und wieder auf die ID-Medien geschrieben werden. Verlorene Medien werden im System gesperrt. Die Sperrung kann mit einem Programmer oder einem ID-Medium an die Offline-Türkomponenten übermittelt werden.

Vor- und Nachteile

- ⊕ Keine Verkabelung notwendig
- ⊕ Geringer Montage- und Installationsaufwand
- ⊕ Einfaches Nachrüsten von Türen
- ⊕ Zutrittsrechte werden auf das ID-Medium geschrieben
- ⊖ Zutrittsrechte sind nicht sofort verfügbar
- ⊖ Kartensperrungen müssen vor Ort auf die Türkomponenten geladen werden und sind erst dann wirksam

Autonome Zutrittskontrolle: Zutrittskontrollzentrale und Leser

Die Zutrittsrechte und Zeitprofile werden mit einer Software zentral verwaltet und mit einem Programmer oder einem Notebook in eine Zutrittskontrollzentrale oder einen Türmanager geladen. Die Zutrittsrechte können verändert oder gelöscht und müssen jeweils wieder in die Zutrittskontrollzentrale geladen werden. Diese Lösung wird bei Schiebetüren oder Türen mit Motorschlössern eingesetzt.

Vor- und Nachteile

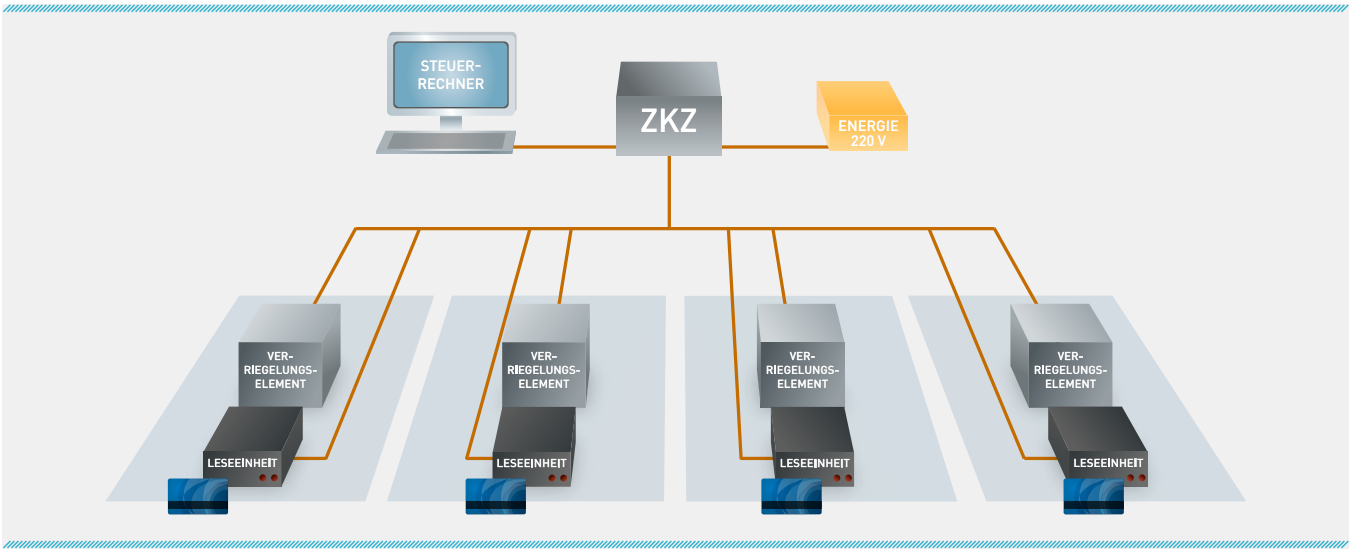
- ⊕ Keine Netzwerkverkabelung notwendig
- ⊖ Zutrittsrechte müssen lokal in der Zutrittskontrollzentrale gespeichert werden
- ⊖ Zutrittsrechte sind nicht sofort verfügbar
- ⊖ Kartensperrungen sind nicht sofort wirksam

Online Zutrittskontrolle: Zutrittsrechte online bei den Türkomponenten

Die Zutrittsrechte und Zeitprofile werden mit einer Software zentral verwaltet und über das IT-Netzwerk in die Zutrittskontrollzentrale geladen. Die Zutrittsrechte können online geändert und verlorene Ausweise sofort gesperrt werden. Die Türsteuereinheiten lassen sich zentral oder dezentral verkabeln. Alle Türsteuereinheiten und Zutrittsleser sind über ein Bussystem mit einer Zutrittskontrollzentrale vernetzt.

Vor- und Nachteile

- Zutrittsrechte sofort verfügbar
- Kartensperrungen sofort wirksam
- Zentrale Türüberwachung möglich
- Ereignismeldungen sofort verfügbar
- Verkabelungsaufwand



Zentrale Installation mit Leser und Verriegelungselementen.

Zentrale Installation

An eine Zutrittskontrollzentrale können mehrere Türen angeschlossen werden. Die Zutrittskontrollzentrale trifft die Zutrittsentscheidungen für alle Türen. Türverriegelungen und Magnetkontakte werden an der Türsteuereinheit oder der Zutrittskontrollzentrale angeschlossen. Nur die Zutrittskontrollzentrale ist über das IT-Netzwerk mit dem Zutrittsserver verbunden.

Je nach Gebäudeart, Anzahl Etagen und somit Distanzen müssen mehrere Zutrittskontrollzentralen eingesetzt werden.

Vor- und Nachteile

- Zentrale Administration
- Verbindungen zu Drittsystemen (EMA, BMA usw.)
- Notstromversorgung der ZKZ
- Installationsaufwand

Dezentrale Installation

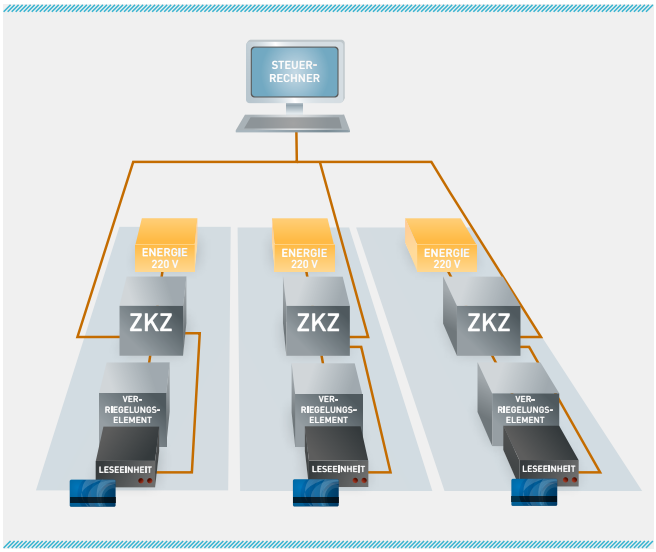
Diese Installationsart ist für kleinere Anlagen geeignet. Wenn ein Netzwerk gewünscht ist, muss die entsprechende Infrastruktur vorhanden sein. Wenn kein IT-Netzwerk vorhanden ist, empfiehlt sich das günstigere Bussystem für die Verknüpfung der einzelnen Elemente. Pro Türe wird eine Zutrittskontrollzentrale installiert, die alle Zutrittsentscheidungen selbstständig trifft. Zutrittskontrollleser, Türverriegelungen und Magnetkontakte werden an diese Zentrale angeschlossen.

Vor- und Nachteile

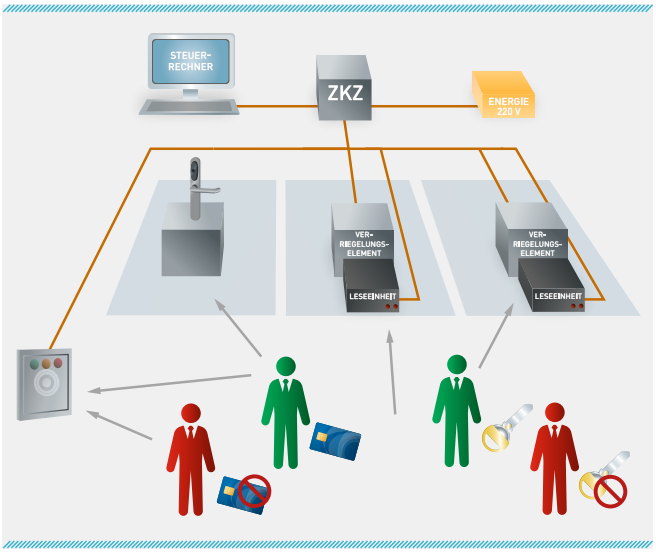
- ⊕ Geringe Installationskosten bei vorhandenem Netzwerk
- ⊕ Zentrale Administration
- ⊖ Notstromversorgung der ZKZ
- ⊖ Verbindungen zu Drittsystemen (EMA, BMA usw.)

Online und Offline heute

Heutige Zutrittskontrollsysteme können Zutrittsrechte sowohl offline wie auch online verwalten. Der Betreiber muss sich nicht für oder gegen eine Lösung entscheiden, sondern er kann von den Vorteilen der verschiedenen Varianten profitieren. Einige Anbieter haben On- und Offline-Systeme im Angebot und können auch mechanische Schliessanlagen verwalten. Andere haben Offline-Lösungen in ihre Systeme integriert. Es wird zwischen einer Teil- und Vollintegration unterschieden. Bei einer Teilintegration wird auf zwei Datenbanken (online und offline) zurückgegriffen, was den Pflegeaufwand etwas erhöht. Eine vollintegrierte Lösung basiert auf einer einzigen Datenbank.



Dezentrale Installation mit Leser und Verriegelungselementen.



Modernes Zutrittskontrollsystem mit Online- und Offline-Angebot.

Einsatzgebiete für Offline/Online

Türen mit organisatorischen Anforderungen an die Zutrittskontrolle werden mit Offline-Lösungen ausgerüstet:

// Türen ohne Türüberwachung, z.B. Bürotüren, Lagerräume
// Türen mit geringer Nutzung, z.B. Putzräume, Abstellräume

Türen mit hohen Sicherheitsanforderungen werden mit Online-Lösungen ausgerüstet:

// Türen mit Türüberwachung z.B. Aussentüren, Etagentüren, Archive, Serverräume usw.
// Türen mit Fernöffnung, z.B. Haupteingänge, Lieferanteneingänge
// Türen mit vielen Änderungen von Zutrittsrechten, z.B. Etagentüren
// Türen mit hoher Nutzung, z.B. Personaleingang, Verbindungstüren

ALS DIE DATEN FLIEGEN LERNTEN

In der Zutrittskontrolle werden nur noch Chipkarten und berührungslose Technologien verwendet. Andere Kartentechnologien (Magnetstreifen, Barcode, Infrarot u.a.) sind noch bei älteren Systemen anzutreffen, wo Medien einmalig verwendet werden oder der Preis ein wichtiges Kriterium ist, z.B. in Bibliotheken, in Messen oder Parkhäusern.

Fragen vor der Wahl der richtigen Technologie

// Wie hoch sind die Anforderungen an die Sicherheit?
// Welches ist der Einsatzbereich?
// Sind bereits Technologien im Einsatz? Müssen alle Applikationen mit ein und derselben Karte benutzt werden können?
// Sind weitere Anwendungen geplant?
// Welche Lesegeschwindigkeiten werden erwartet?
// Müssen Daten auf dem Medium gespeichert werden und wie gross ist der Speicherbedarf?
// Welche Lesedistanzen sollen möglich sein?
// Wird das Medium von einer Person oder einem Gerät geprüft?

Chipkarten

Ausweise mit kontaktbehaftetem Chip eröffnen vielfältige Möglichkeiten für Codierung und Sicherheit und werden hauptsächlich für den Zugriff auf den PC-Arbeitsplatz verwendet. Die Speicherkapazität ist hoch und die Gefahren von Veränderung, Verfälschung und Nachahmung können durch organisatorische Massnahmen so gut wie ausgeschlossen werden. Die Chips sind mit Kontakten ausgestattet, deren Position in einer ISO-Norm festgelegt ist. Dafür sind aufwändige Einsteckleser erforderlich, welche die Kontaktfühler im Leser mit den Kontaktflächen auf der Karte zusammenzubringen müssen.

RFID-Verfahren

Die **R**adio **F**requency **I**dentification (Funktechnologie) basiert auf elektromagnetischen Wellen und ermöglicht die automatische Identifizierung und Lokalisierung von Gegenständen und erleichtert die Erfassung von Daten wesentlich. Ein RFID-System besteht aus einem Transponder, der sich in einem Gegenstand befindet (z.B. Ausweiskarte) und einen kennzeichnenden Code enthält sowie einem Lesegerät zum Auslesen dieser Kennung. Man spricht dabei von der Proximity- oder Näherungs-Lesung mit Lesedistanzen von max. 10 cm. Für grössere Distanzen (z.B. LKWs, Stapler) gibt es Systeme mit höherer Frequenz und eigenen ID-Medien.

In der Schweiz sind Legic (LEGIC Identsystems AG, Tochtergesellschaft von KABA) und mifare (NXP, Spin-off von Philips) die häufigsten Technologien im Bereich der Zutrittskontrolle. Weitere Anwendungsgebiete sind möglich:

// IT-Zugang
// Büroautomationen (Freigabe von Druckern und Kopierern)
// Zeit- und Leistungserfassung
// eTicketing (Konzerte, Sportveranstaltungen usw.)
// ePayment (Cash, Vending, Catering-Lösungen usw. für die Bezahlung an Automaten und Kassen)
// Parking-Lösungen usw.

Near field communication NFC

NFC ist ein internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten per Funktechnik über kurze Strecken von wenigen Zentimetern. Dabei werden Applikationen und Rechte via GSM und Internet übermittelt. Das ist dann von Vorteil, wenn Rechte kurzfristig und für räumlich weit auseinander liegende Objekte vergeben werden müssen.

Resistive Capacitative Identification RCID

Im Gegensatz zur RFID nutzt RCID nicht elektronmagnetische, sondern für den Körper völlig harmlose elektrostatische Felder. Dabei wirkt dieser als Übertragungsmedium: Trägt man einen Sender auf sich (z.B. in der Hosentasche) und berührt einen Empfänger (z.B. Türgriff, oder Fussmatte), schliesst sich der Kreis und die Identifikation findet statt.

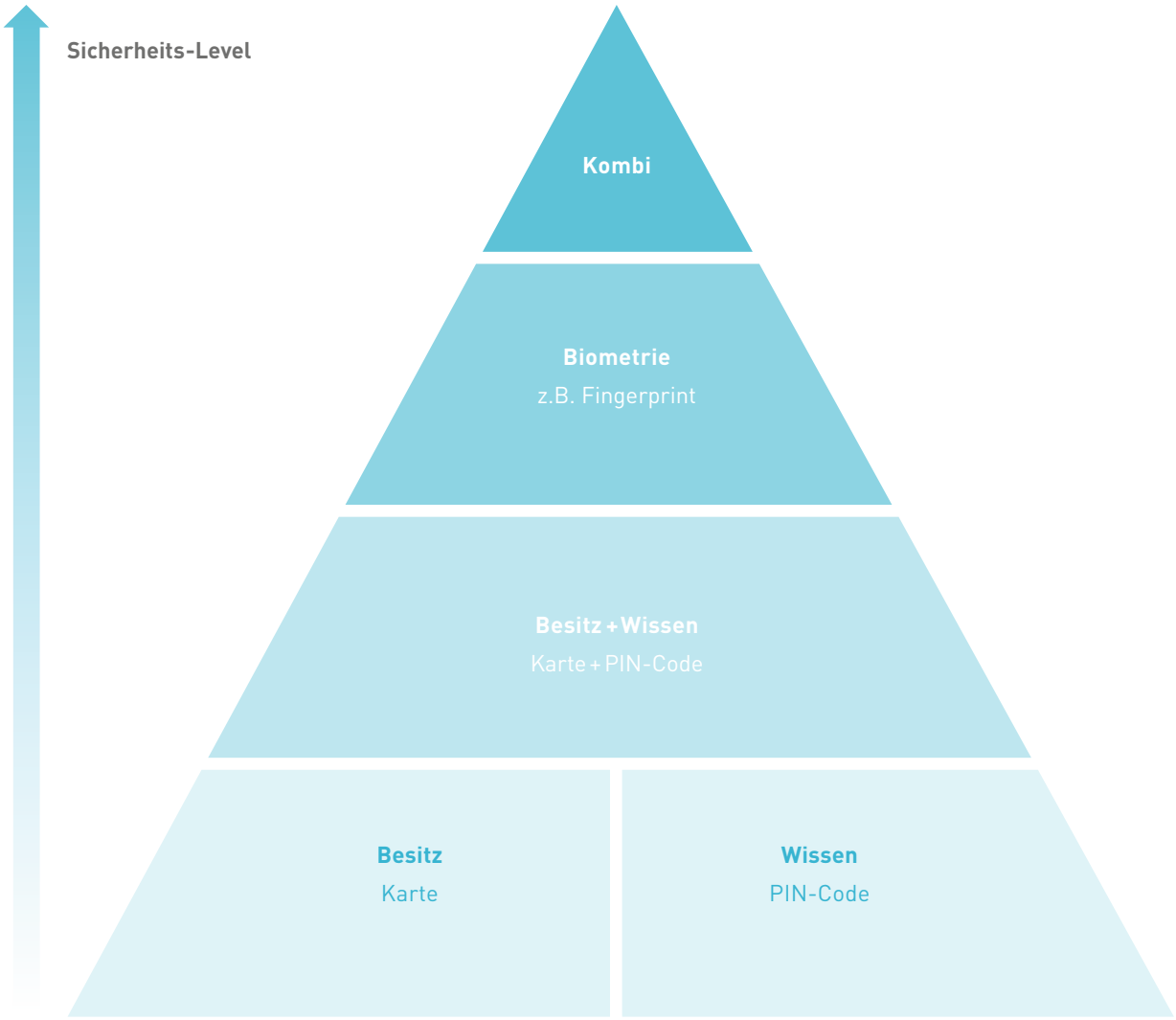
Übertragungs- und Datensicherheit

Bei all diesen Applikationen muss geklärt werden, ob die Daten auf der Karte oder zentral gespeichert werden sollen. Beide Lösungen haben ihre Vor- und Nachteile. Werden die Daten auf der Karte abgelegt, ist die Verlustgefahr grösser; dafür kommt diese Methode bei Biometrie-Anwendungen zum Einsatz, weil die sensiblen Daten beim Eigentümer bleiben. Sollen die Daten hingegen in einem zentralen System verwaltet werden, empfiehlt sich die (eher aufwändige) Vernetzung aller Lesegeräte.

Speziell bei Lösungen für die bargeldlose Zahlung mit verschiedenen Lieferanten und allenfalls mehreren Standorten ist zu beachten:

// Kann eine einheitliche Datenstruktur verwendet werden?
// Haben alle Partner eine Lese-/Schreibeinheit für eine solche Lösung?
// Soll das «Geld» auf der Karte liegen?
// Wer ist für das Clearing unter den verschiedenen Lieferanten verantwortlich?
// Wie werden Lesegeräte zum Pool hinzugefügt?

Die Sicherheit eines Zutrittskontrollsystems kann den Anforderungen des Nutzers angepasst werden. Werden nur der Besitz (eines Mediums) oder das Wissen geprüft, ist die Sicherheit tief. Das Wissen kann einfach weiter gegeben oder ausspioniert, das Medium weitergegeben oder gestohlen werden. Die Kombination dieser Verfahren führt zu einer deutlichen Steigerung der Sicherheit. Wissen und Besitz sind jedoch nicht an eine Person gebunden, die Sicherheit nur so gut wie der Umgang damit. Die Biometrie schliesslich bietet die höchste Sicherheit, weil personengebundene Merkmale weder weitergegeben oder ausspioniert noch gefälscht werden können.


Sicherheits-Level
Kombi
Biometrie
z.B. Fingerprint
Besitz + Wissen
Karte + PIN-Code
Besitz
Karte
Wissen
PIN-Code

SESAM ÖFFNE DICH!

Werden nur das Wissen (PIN) beziehungsweise biometrische Merkmale geprüft, ist kein Medium notwendig. Häufig macht jedoch eine Kombination von zwei oder drei Verfahren Sinn. Wir stellen die am häufigsten eingesetzten Medien kurz vor.

Karte

Die üblichste Bauform (im Kreditkartenformat) und bestens geeignet als gleichzeitiger Sichtausweis.

Der moderne Vollplastikausweis ist ein Laminat aus verschiedenen, sehr dünnen Einzelfolien. Diese werden mit dem erforderlichen Inlay (z.B. Chip mit Antenne) und dem Deckblatt zusammengeschweisst.

Der Gestaltung und Bedruckung von Plastikausweisen sind fast keine Grenzen gesetzt. Dabei können Firmenlogos, Mitarbeiterfotos, aber auch Sicherheitselemente wie Hologramme aufgebracht werden. Mit speziellen Ausweisdruckern für Offset- und Thermodruckverfahren können die Karten unabhängig vom Lieferanten ausgegeben werden.

Schlüssel

Die Integration von RFID-Komponenten in den Schlüssel ist bei mechatronischen Lösungen praktisch, d.h. das Nebeneinander von berührungslosen Lesern und herkömmlichen, mechanischen Zylindern. Allerdings ist die Lesedistanz eingeschränkt.

Schlüsselanhänger / Armband

Robuste Variante, allerdings mit geringerer Lesedistanz als die Karte.

Folgende Fragen können bei der Evaluation der richtigen Bauform helfen:

// Soll der Ausweis individualisiert werden können (z.B. Firmenerscheinungsbild)?
// Müssen weitere Sicherheitsmerkmale aufgebracht werden (z.B. Hologramm)?
// Muss das Medium berührungslos und auf möglichst grosse Distanz gelesen werden können?
// Soll das Medium auch als Schlüssel dienen?
// Muss das Medium sehr robust sein (mechanische Belastung, Feuchtigkeit, Temperatur)?

Lesegeräte

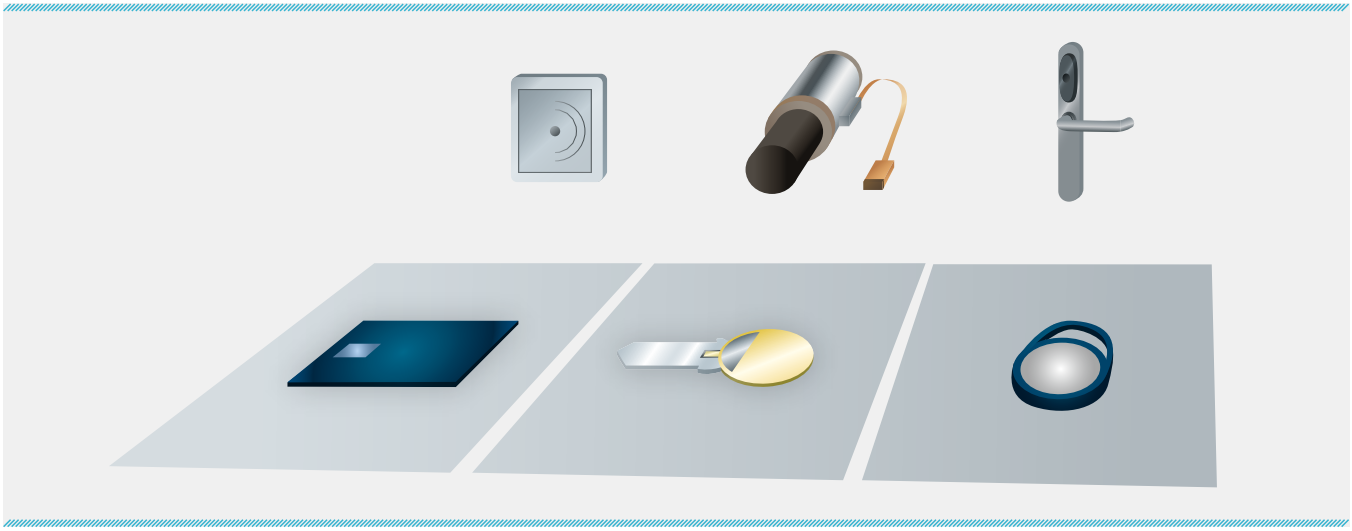
Der Leser (auch Leseeinheit oder Sensor) erfasst die Identifikationsmerkmale des Benutzers und übermittelt sie an die Zentrale. Der Benutzer kann sich durch Besitz (z.B. einer Karte, eines Tags), durch Wissen (einer PIN oder Kennzahl), physische Merkmale (Biometrie) oder eine Kombination davon ausweisen. Jedes dieser Verfahren hat eine mehr oder weniger hohe Sicherheitsstufe.

Leser gibt es in den verschiedensten Ausführungen und Designvarianten mit folgenden Unterscheidungskriterien:

// Mit/ohne Tastatur
// Lesertechnologie (LEGIC, mifare, EM, Hitag usw.)
// Lesedistanz
// Vandalensicherheit
// Schutzart nach IP (Innen-/Ausseneinsatz)
// Mit/ohne Display (Terminal z.B. auch für Zeiterfassung)
// Stand-alone-Betrieb möglich
// Integration in Zylinder, Türbeschlag

Mit oder ohne Tastatur

Die RFID-Leseeinheiten können mit einer Tastatur ausgerüstet werden, über die eine PIN (Persönliche Identifikations-Nummer) eingegeben wird. Durch diese Kombination werden also Besitz und Wissen geprüft. Eine Kombination mit biometrischen Systemen zur Erhöhung der Sicherheit ist ebenfalls möglich.



Die häufige Verwendung der Tasten kann, je nach Qualität, zu Verschleisserscheinungen führen. Unter diesen Umständen lassen sich PIN-Codes recht einfach ausspionieren. Für Hochsicherheitsanwendungen sind sogenannte Scramble Code-Leser erhältlich, bei denen die Position der Zahlen nach jeder Eingabe nach dem Zufallsprinzip ändern.

Für die unterschiedlichen Anwendungen sind entsprechende Bauformen verfügbar. In der Schweiz hat sich Feller-Edizio als Quasi-Standard durchgesetzt. Bei industriellen Anwendungen haben sich Aufputzmodelle, optional mit Schlag- und Spritzwasserschutz, etabliert. Auch die Kombination mit Türsprechstellen und Portraitkameras ist möglich.

Offline-Leser

Es gibt auch Lesegeräte, die nicht in ein Netzwerk eingebunden sind und somit nicht mit einem zentralen Rechner kommunizieren. Die sogenannten Beschlagsleser eignen sich für Einzeltüren ohne Sicherheitsanforderung oder wenn der Einsatz von mechanischen Schlüsseln nicht erwünscht ist.

Der Einsatz von Beschlagslesern an Brandschutz- und Fluchttüren ist unbedingt von den entsprechenden Behörden genehmigen zu lassen.

HIER GEHT'S ANS LEBENDIGE

Die Biometrie beschäftigt sich mit unverwechselbaren physiologischen und verhaltenstypischen Merkmalen von Lebewesen (z.B. Finger, Hand, Augen) und den dazu erforderlichen Mess- und Auswerteverfahren. Der Einsatz von biometrischen Identifikationsverfahren in der Zutrittskontrolle soll sicherstellen, dass nur diejenige Person Zutritt erhält, die auch die entsprechenden Merkmale besitzt. Der Betrug mit gestohlenen Ausweisen beispielsweise wird dadurch stark erschwert oder verhindert.

Bei der Personenidentifikation gehören biometrische Verfahren zu den wichtigsten automatisierbaren Authentifikationsmethoden. Authentifikation bedeutet «Bezeugung oder Verifikation der Echtheit.» Während traditionelle Authentifikationstechniken wie PIN-, Passwort- oder Smartcard-Verfahren (Chipkarte) auf der Verifikation durch Wissen oder durch Besitz beruhen (vgl. S.16), benutzt die Biometrie mit physiologischen und verhaltenstypischen Charakteristiken daher personengebundene – und nicht nur personenbezogene – Merkmale.

Bei der Auswertung wird zwischen Identifikation und Verifikation unterschieden:
Identifikation bedeutet «Feststellung der Identität.» Die biometrischen Merkmale einer Person werden mit allen in der Datenbank gespeicherten Referenzdaten verglichen. Es erfolgt ein 1:1-Vergleich mit einer Vielzahl von Datensätzen. Je mehr Referenzdatensätze im System gespeichert sind, desto länger dauert die Identifikation.

Verifikation bedeutet «Bestätigung der Identität». Bei einer Verifikation wird in einem 1:1-Vergleich geprüft, ob eine behauptete Identität bewiesen werden kann. Eine Person gibt sich z.B. mit Karte oder PIN zu erkennen. Danach vergleicht das System seine Biometrie-Daten (Template) mit der Sensormessung. Dieses Verfahren ist schneller und sicherer als die Identifikation. Ist das Referenz-Template sogar auf einer Karte gespeichert, muss keine zentrale Datenbank geführt werden, ein grosser Vorteil aus Sicht des Datenschutzes.

Die Anschaffungskosten für einen Biometrie-Leser sind meist höher als für ein RFID-Gerät. Diese werden allenfalls durch den Wegfall der Beschaffung und Verwaltung von RFID-Karten etwas relativiert.

Anforderungen an biometrische Merkmale

Ein biometrisches Merkmal sollte zumindest die folgenden Eigenschaften erfüllen:

- Unterscheidbarkeit/Einzigartigkeit (Distinctiveness); unterschiedliche Ausprägung von einem Individuum zum andern.
- Universalität/Verbreitung (Universality); etwas, über das jeder Mensch verfügt.
- Dauerhaftigkeit/Konstanz (Permanence); etwas, das sich bei jedem Individuum nicht verändert. Adaptive (anpassungsfähige) Verfahren können kleinere Veränderungen (z.B. leichte Verletzung am Finger) ausgleichen.
- Zugänglichkeit/Erfassbarkeit (Collectability); etwas, von dem sich leicht ein Abbild erstellen lässt.

Folgende Eigenschaften sind zudem wünschenswert:

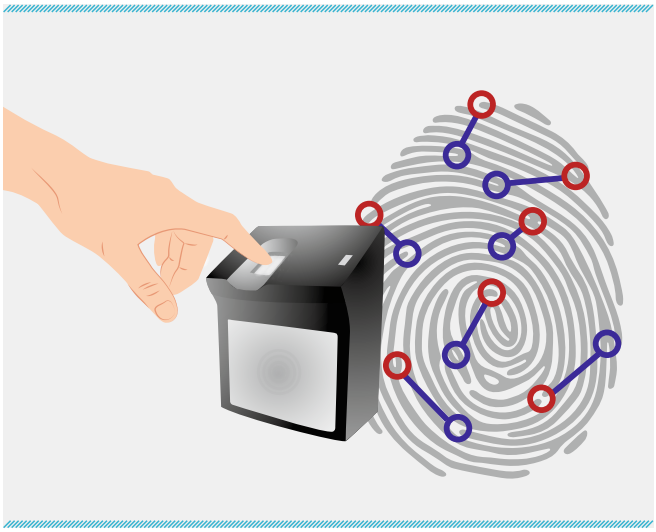
- Leistungsstärke (Performance); robust, genau, wirkungsvoll und rasch analysierbar.
- Akzeptanz (Acceptance); kein Widerstand gegen das Sammeln der Daten.
- Zuverlässigkeit (Reliability); damit Fälschungen und die Umgehung der Vorweisung erschwert werden.

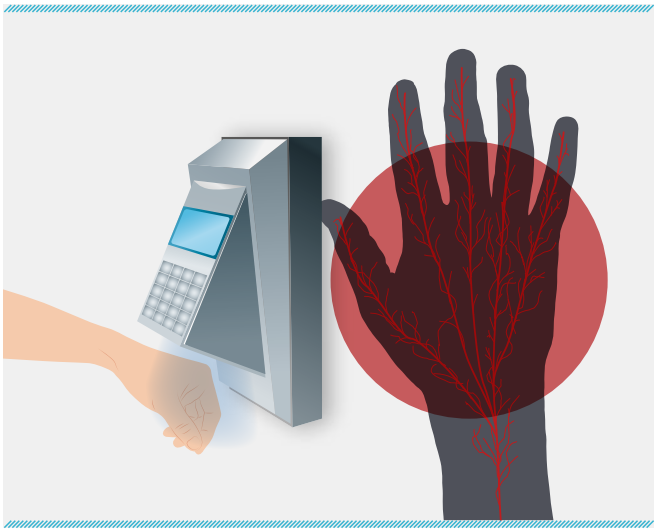
Zwei Verfahren

Die biometrische Erkennung wird grundsätzlich in zwei Gruppen unterteilt:

- Physiologische Charakteristika (auch als «passive Merkmale» bezeichnet): Fingerabdruck, Venenmuster, Handgeometrie, Augen (Retina, Iris), Gesicht.
- Verhaltensspezifische Charakteristika (auch «dynamische Merkmale»): Unterschrift, Stimmbild, Gangart, Art des Tastenschreibens.

Die Auswertung von verhaltensspezifischen Merkmalen sind eher im Komfortbereich anzusiedeln (Sprachsteuerung von Geräten usw.) In der Zutrittskontrolle werden vor allem Systeme eingesetzt, welche die statischen Merkmale auswerten. Es sind selbstverständlich auch Merkmalskombinationen sinnvoll, z.B. Gesichts- und Stimmenerkennung.





Fingerabdruck

Insgesamt verfügt der Fingerabdruck über zirka 35 unterschiedliche Ausprägungen (Minutien) wie Kreuzungen, Endungen, Verzweigungen oder Punkte. Für eine eindeutige Identifikation genügt es in der Regel, 8 bis 22 Merkmale sowie deren Distanz und Lage zueinander zu überprüfen.

Vor- und Nachteile

- ⊕ Geringer Speicherbedarf des Template
- ⊕ Günstig
- ⊖ Temperaturabhängig
- ⊖ Benutzer können Vorbehalte haben bezüglich der Hygiene
- ⊖ Einschränkung bei fehlendem oder schwachem Fingermuster

Gefässstruktur im Handrücken

Das System erkennt den individuellen Verlauf der Venen und arbeitet mit einem spezifischen Erkennungsalgorithmus, der durch Infrarot-Technologie extrahierte Handgefässstruktur erkennt und verarbeitet. Selbst bei eineiigen Zwillingen unterscheidet sich das Muster, das nicht durch die DNA bestimmt wird.

Vor- und Nachteile

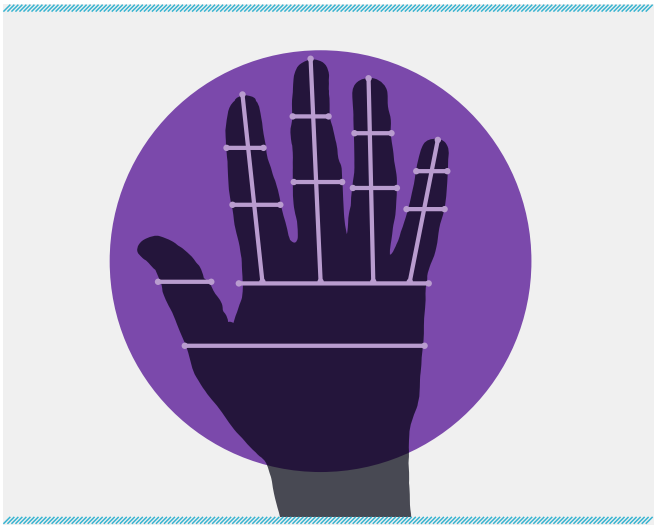
- ⊕ Der Zustand der Hautoberfläche hat keinen Einfluss auf das Template, die Messung erfolgt subkutan.
- ⊕ Kleinere Verletzungen sowie Schmutz provozieren keinen Erkennungsfehler.
- ⊕ Keine Enrollment-Ausfälle, da jeder Mensch ein Venenmuster besitzt.
- ⊕ Die Position der Venen bleibt zeitlebens unverändert und ist bei jedem Menschen unterschiedlich.
- ⊖ Temperaturabhängigkeit

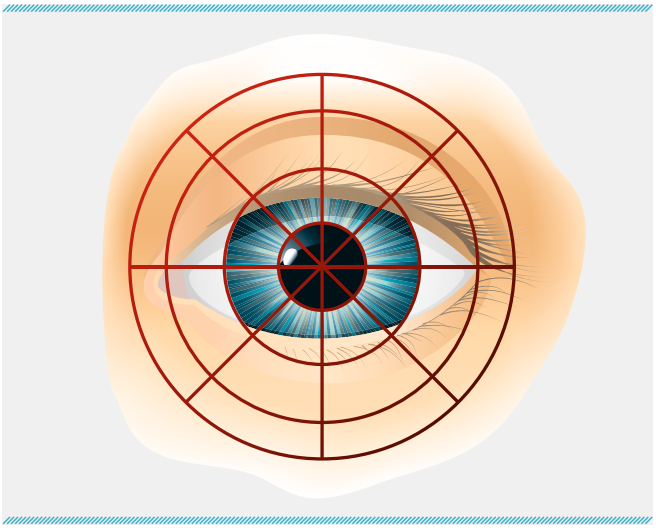
Handgeometrie

Wie bei der Gesichtserkennung verwendet auch das Handgeometrie-Verfahren ein optisches System in Form einer Kamera, um die spezifischen Merkmale einer Hand abzubilden. Dabei werden ebenfalls der Handrücken und über Spiegel die Seitenansicht der Hand optisch aufgenommen und ausgewertet.

Iris

Die Augeniris oder Regenbogenhaut ist die durch Pigmente gefärbte Blende des Auges. Sie ist das komplexeste Merkmal des menschlichen Körpers, welches für die biometrische Analyse geeignet ist. Sie entsteht zufällig und wird nicht von der Erbmasse beeinflusst. Die Iris umfasst mit ihren Punkten, Sprenkeln, Streifen und Fäden insgesamt 266 biologische Merkmale.





Speicherung biometrischer Daten (Merkmale)

Die Speicherung der Referenzdaten erfolgt entweder zentral im Zutrittskontrollsystem oder direkt auf dem Ausweis. Ist das Referenz-Template auf einer Karte gespeichert, muss keine zentrale Datenbank geführt werden, was aus Sicht des Datenschutzes einen grossen Vorteil bedeutet.

Toleranz des Systems

Bei jedem Zutrittsbegehren wird ein neuer Merkmalsvektor erstellt, der mit dem gespeicherten verglichen wird. Da jede Messung zu leicht unterschiedlichen Ergebnissen führt (Auflagewinkel und -druck, körperliche Aktivität, Temperatur, Feuchtigkeit usw.), muss das System mit einer gewissen Abweichung zum Referenzdatensatz umgehen können.

Sicherheit vs. Komfort

Es stellt sich grundsätzlich die Frage, inwiefern zugunsten der Sicherheit auf eine schnelle, einfache, günstige und komfortable Prüfung verzichtet werden soll.

Der Einsatz der Biometrie stellt sicher, dass das Individuum, und nicht nur der Besitz oder das Wissen, geprüft wird. Gleichzeitig bietet es zusätzlichen Komfort, weil kein Ausweis verloren oder keine PIN vergessen geht. Die Erfassung des biologischen Merkmals kann sogar berührungsfrei, sprich «freihändig» erfolgen.

Fazit: Der Betreiber wählt die Technologie, den Einsatz und das Verhältnis von Komfort und Sicherheit.

Ein Nachteil von biometrischen Systemen ist, dass sie nicht bei allen Personen funktionieren. Ein Fingerprint-Leser kann z.B. bei Menschen versagen, die nur schwach ausgeprägte (Kinder) oder keine Fingermuster (nach Verletzung) haben, d.h. ca. 4–5% der Menschen. Für diese Fälle sollte ein Szenario mit alternativem Zutritt (Degrading) entwickelt werden, z.B. nur mit Karte oder PIN.

Biometrische Systeme erfordern die Zustimmung der Benutzer.
Es gilt, Ängsten und Zweifeln mit gezielter Information und Schulung entgegenzuwirken.

Bedenken und Unsicherheiten

Folgende Massnahmen und Argumente können helfen, Zweifel zu beseitigen.

Datenschutz

- Das Speichern der Templates auf einer Karte und eine gesicherte Datenübertragung können der Missbrauch weitest gehend eliminieren.
- Mit den gespeicherten Daten (Template) darf der Finger oder das Gesicht nicht rekonstruiert werden können.
- Die Templates dürfen nicht für den Nachweis von Krankheiten verwendet werden können.
- DieTemplates sollen verschlüsselt abgelegt werden.
- Der Zugriff auf die Templates muss klar geregelt sein.

Gesundheit

- Zur Iriserkennung wird nicht, wie oft vermutet wird, ein Laser, sondern eine Kamera eingesetzt.

Fragen bei der Evaluation biometrischer Systeme

- Welche Ziele sollen mit einem biometrischen Erkennungssystems erreicht werden?
- Handelt es sich um eine biometrische Identifikation oder Verifikation?
- Welches Messverfahren soll angewendet werden?
- Welches sind die Rechtfertigungsgründe für die Datenbearbeitung?
- Wie viele Personen werden registriert?
- Sollen die biometrischen Daten zentral oder dezentral gespeichert werden?
- Bei dezentraler Speicherung: Nach welchem Verfahren?

TÜR UND TOR ÖFFNEN – UND ÜBERWACHEN

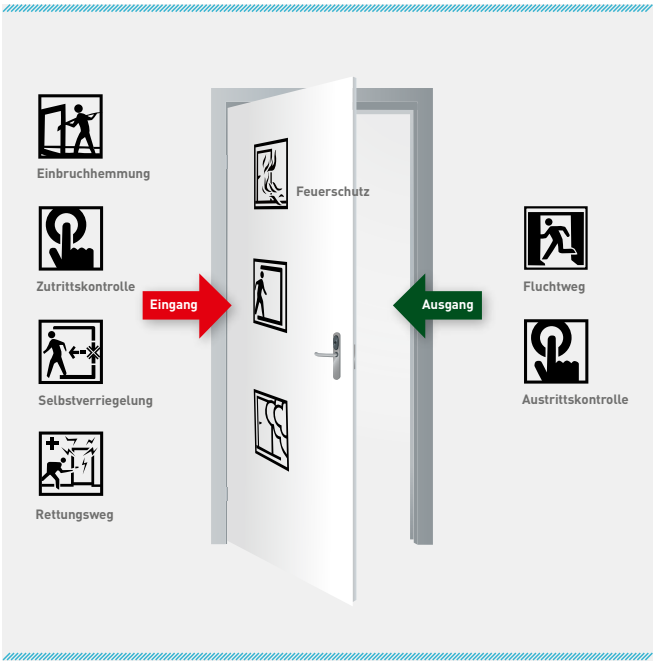
Es liegt nahe, dass ein Zutrittskontrollsystem mit der Steuerung von Türen, Toren und Schleusen sowie Alarmierungs-Produkten gekoppelt wird. Dazu sind spezielle Türkontroller und Türkomponenten erhältlich. Die Türmanager steuern und überwachen jeweils selbstständig eine oder mehrere Türen inklusive Leser.

Ein Türmanager ist nur so gut wie seine Türen und die Sicherheitskomponenten. Je nach Frequentierung können mehrere hundert Begehungen pro Tag erfolgen, was eine enorme Belastung der mechanischen und elektromechanischen Teile bedeutet. Weitsichtige und gründliche Planung unter Beizug aller Spezialisten kann verhindern, dass sie frühzeitig versagen oder die Sicherheit nicht gewährleisten. Zudem müssen die Schutzfunktionen der Türen, z.B. gegen Einbruch, Brand und Schall, aber auch die Fluchtweggestaltung genau bedacht werden. Dazu sind die umfangreichen gesetzlichen Normen zu beachten.

Ein kurzer Blick auf die unterschiedlichen Arten von Türen und Durchgängen dient als Einstieg in dieses Thema.

Türtypen

Flügeltüren	Zur Abgrenzung von Innen- und Aussenräumen; Verriegelung mit einem Schloss.
Schiebetüren	Ein Türblatt/mehrere Türblätter, oben oder unten geführt, seitlich öffnend.
Drehtüren	Zwei oder vier rotierende Türflügel in einem runden Gehäuse für gleichzeitigen Ein- und Ausgang.
Drehsperren	Fix montiertes Gehäuse mit drei Holmen für den Einzelzugang.
Drehkreuze	Zwei, drei oder vier vertikal geführte Flügelrechen für die sogenannte Vereinzelung von grösseren Menschenmengen.
Sensorschleusen	Sensorisch überwachter Durchgang mit Schiebe- oder Schwenktüren.
Personenschleusen	Kabinen mit zwei gegenüberliegenden Türen/Schiebetüren als Vereinzelungsmassnahme.



Türöffner

Ein Türöffner ist eine im Türrahmen eingebaute Vorrichtung, mit elektromagnetischer Entriegelung der Schlossfalle.

Es wird unterschieden zwischen

- Standardtüröffner, aufbruchsicher von 3 500 bis 5 000 N
- Sicherheitstüröffner, aufbruchsicher von 3 000 bis 15 000 N
- Fluchttüröffner, sicheres Entriegeln auch bei Fallenvorlast
- Modell «Silence» ohne Klickgeräusch für Spitäler und Heime
- Funkschloss zur Ansteuerung über Handsender

Sicherheitsschloss

Ein besonders gesichertes (Tür)Schloss mit einem durch mehrere Stifte festgehaltenen Zylinder.

Selbstverriegelndes Schloss

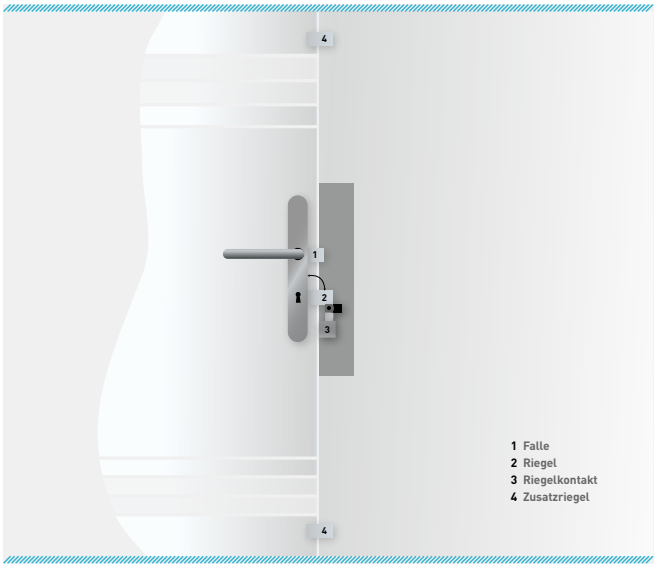
Sofort nach jedem Schliessen der Tür schiebt sich der Riegel automatisch wieder vor.

Mehrfachverriegelung

Sicherheitsschloss mit Mehrpunkteverriegelung, in der Regel drei, mit erschwertem Aushebeln durch mechanische Kräfte.

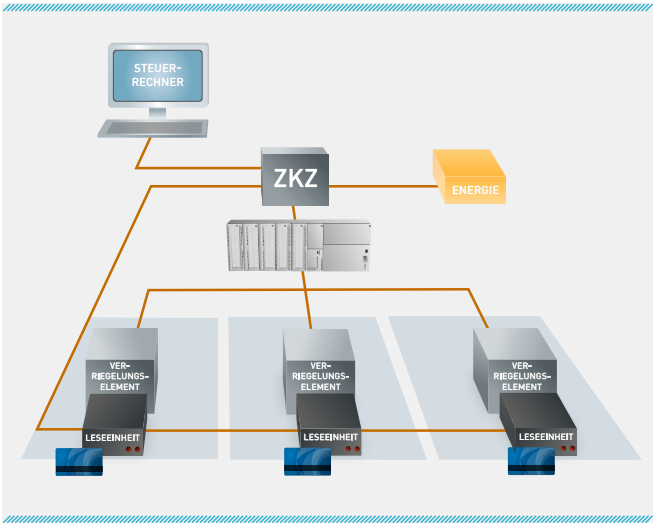
Rückmeldekontakte

Für die Zustandsüberwachung von Türen (geschlossen, verriegelt, offen) kommen vorwiegend Magnetkontakte, aber auch Riegelkontakte zum Einsatz.

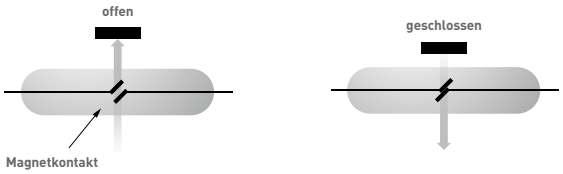


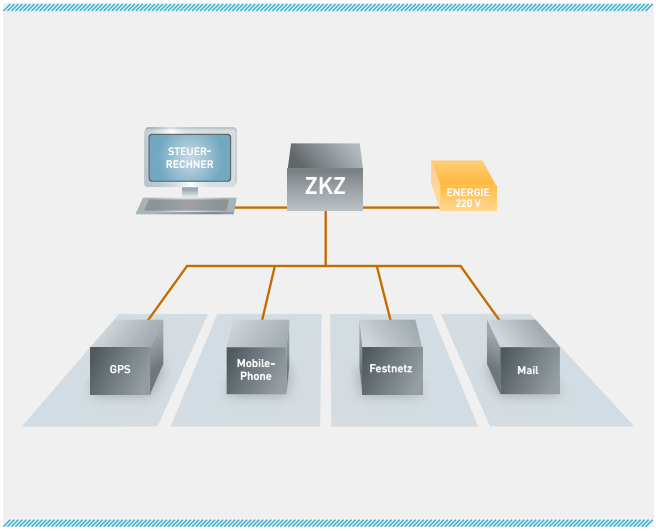
Türmanagementsysteme

Bei komplexen Installation werden die Türkomponenten nicht mehr von einem Türkontroller bearbeitet, sondern an ein übergeordnetes Tür-Management-System (TMS), wie z.B. eine Speicher-Programmierbare-Steuerung (SPS), weitergeleitet. Sie löst zusehends die «festverdrahtete» verbindungsprogrammierte Steuerung ab. Sensoren, d.h. Türkontakte, Lichtschranken usw. sowie Aktoren (Türöffner, elektrische Schlösser u.a.) werden direkt an die SPS angeschlossen. Ob als zentrale Baugruppen oder als modulare Lösung mit dezentralen Modulen, garantiert die SPS eine hohe Flexibilität und Erweiterbarkeit. Die Schnittstelle zur Zutrittskontrolle kann eine digitale sein.



Einige Systeme haben eine serielle Schnittstelle integriert und können so auf die aufwendige Verdrahtung verzichten. Beim Einsatz von mehreren SPS-Modulen werden diese über das Netzwerk (Ethernet) miteinander verbunden, was die Flexibilität und Geschwindigkeit zusätzlich erhöht.





Überwachung und Alarmierung

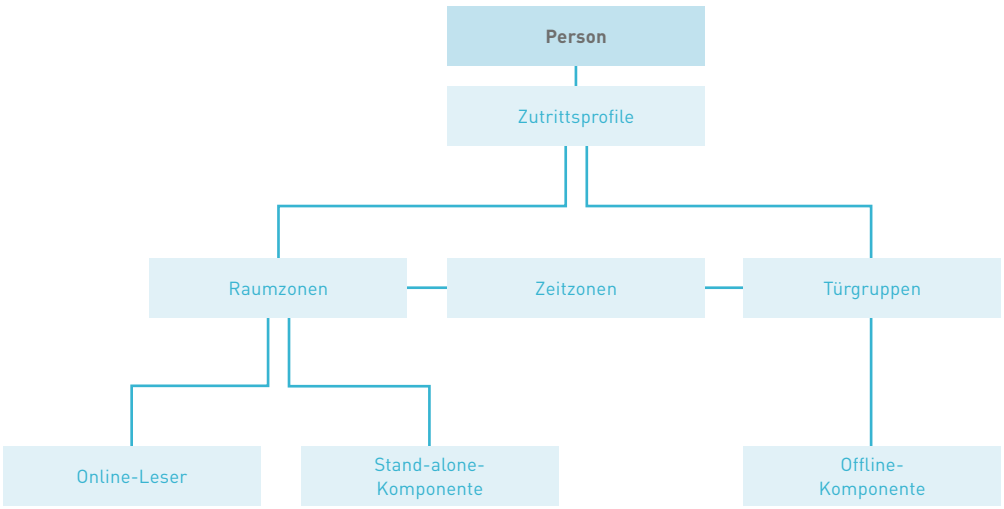
Zur Veranschaulichung dieses Bereichs dient die Ereigniskette bestehend aus Detektion, Übermittlung, Verarbeitung und Intervention.

Detektion Meistens sind dies Sensoren wie Brand- und Einbruchmelder, Türkontakte (vgl. oben), Gasmelder, Störkontakte von technischen Systemen u.a.

Übermittlung Die Alarmübermittlung erfolgt häufig über einen sog. Alarmserver (PC), der die Alarme an beliebige Endgeräte wie Pager, Telefone, Handys oder an Mailadressen weiterleiten, immer häufiger über Internet.

Verarbeitung Bei erhöhten Sicherheitsanforderungen empfiehlt sich die Alarmweiterleitung an spezialisierte Empfangsstellen, weil die Verfügbarkeit und die Infrastruktur gewährleistet sind.

Intervention Je nach Ereignis bietet die Alarmempfangsstelle den Eigentümer, Servicetechniker, Sicherheitsdienst, die Polizei, die Feuerwehr u.ä. auf.



VON RECHTEN UND PFLICHTEN

Die verschiedenen Anbieter haben unterschiedliche Ansätze für die Abbildung von Berechtigungen im System. Eines ist jedoch allen gemeinsam: Sie zeigen wer (Medium) wann wohin darf.

Da die Umsetzung der Rechtevergabe so individuell ist wie das System, sollte der Nutzer dem Anbieter seine Bedürfnisse klar darstellen. Das Konzept muss dann gemeinsam erstellt werden. Nach der Einführung sollte der Betreiber in der Lage sein, das Modell sinnvoll zu erweitern und die Rechtevergabe selbstständig vorzunehmen.

Zutrittssperren

Die Zutrittswiederholsperre (auch Zutrittswiederholkontrolle genannt) verhindert, dass mit demselben Medium ein Zutritt in eine Zone erneut erfolgen kann, ohne vorherigen Austritt. Eine Variante davon ist die zeitliche Beschränkung dieser Sperre, nach deren Ablauf der Zutritt zur gleichen Zone erneut möglich ist, auch wenn zuvor kein Austritt protokolliert wurde.

Schleusensteuerungen

In einer Schleuse (z.B. ein Raum oder eine Kabine) dürfen sich nur berechtigte Personen aufhalten. Sie muss durch mindestens zwei Zutrittsterminals abgesichert sein. Wird ein Raum als Schleuse zu anderen Sicherheitsbereichen genutzt, darf er nicht durch mehr als eine Tür gleichzeitig betreten bzw. verlassen werden. Eine Buchung ist nur dann möglich, wenn alle Türen der Schleuse geschlossen sind oder wenn eine Zutrittsbuchung beendet ist.

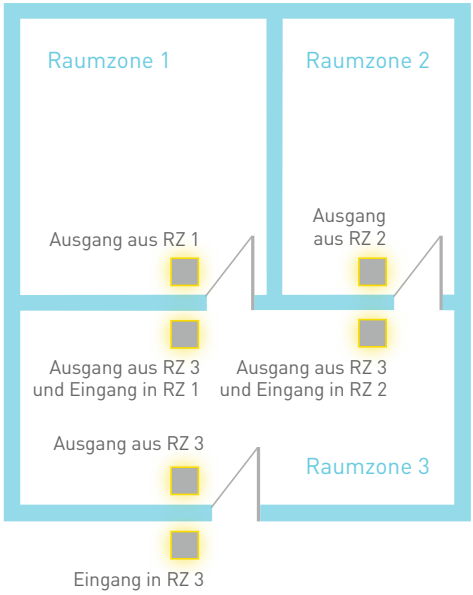
Eine Schleuse kann auch zur Personenvereinzelung genutzt werden. In diesem Fall darf keine Türe zu diesem Raum geöffnet werden, bis die berechtigte Person den Raum (Schleuse) verlassen hat. In der Regel wird eine Zeitlimite hinterlegt, nach deren Überschreitung die Person in die Zone zurück muss, aus der sie gekommen ist.

Beim Einsatz von Schleusen zu beachten

// Die Zuständigkeiten der einzelnen Überwachungssysteme (Einbruch, Brand, Video, Zutritt) müssen klar vergeben werden.
// Notaustritt nicht vergessen!
// Der Betrieb einer Schleuse braucht viel Strom. Auch bei einem Stromausfall müssen alle nötigen Komponenten zuverlässig funktionieren.
// Personenvereinzelungen sind teuer und sollten von Spezialisten geplant werden.
// Schleusen sollten regelmässig gewartet werden. Die Komplexität erfordert ein exaktes Zusammenspiel aller Komponenten.
// Schleusen schränken den Personendurchsatz massiv ein. Bei der Planung müssen die zu erwartenden Personendurchtritte berücksichtigt werden.
// Wie erfolgt der Warentransport resp. der Transport von persönlichen Gegenständen (Koffer, PC usw.)?

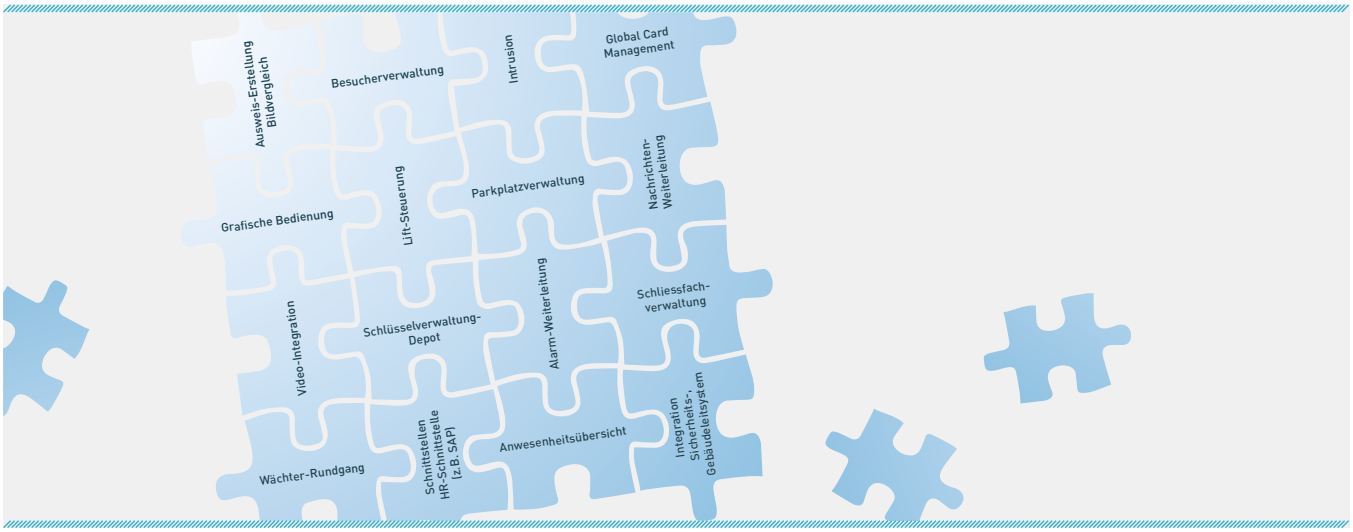
Raumzonenwechsel-Kontrolle, Bilanzierung

Raumzonen sind Teilbereiche eines Sicherungsbereiches, die aus einem oder mehreren Räumen mit einem oder mehreren Ein- und Ausgängen bestehen. Ein Person kann sich immer nur in einer Raumzone aufhalten. Die Raumzonenwechsel-Kontrolle verhindert den Zutritt zu einer benachbarten Raumzone, wenn der Zutrittsberechtigte in der Raumzone, in der er sich befindet, als «nicht anwesend» erfasst ist.



Alle Leser der gleichen Raumzone können zu einer Gruppe zusammengefasst werden. Der Raumzone können weitere Attribute zugeordnet sein:

// Aktuelle Personenanzahl, die sich aktuell in der Raumzone befindet.
// Maximale Personenanzahl, die eine Raumzone betreten darf. Ist das Maximum erreicht, muss eine Person die Zone verlassen, bevor eine andere eintreten kann.
// Minimale Personenanzahl, die sich in einer Raumzone aufhalten muss.
// Maximale Zeit, während der sich Personen in der Raumzone aufhalten dürfen.
// Zeitzone, während der die Zutrittsberechtigung zu einer Raumzone gilt.
// Raumzone leer/nicht leer; je nach Vorgabe wird ein Alarm ausgelöst
// Raumzonenverletzung; der Eintritt kann trotz Zonenverletzung möglich sein, diese wird aber protokolliert oder löst einen Alarm aus.



WAS DIE ZUKO SONST NOCH KANN

Integrationsmöglichkeiten

Systeme und Module können mit der Zutrittskontrolle verschieden interagieren. Dabei wird das Mass der Integration unterschieden.

// Vollintegration: Die Applikation der Zutrittskontrolle wird erweitert, der User benutzt die Erweiterung wie die Stammapplikation.
// Teilintegration: Eine meist schon bestehende Drittapplikation wird mit der Zutritts-Stammapplikation kombiniert.
// Software-Schnittstellen: Bei einer solchen Minimalanbindung, z.B. über WebService, müssen die gemeinsamen Daten nur in einer Applikation gepflegt werden.
// Hardware-Schnittstellen: Über HW-Schnittstellen können verschiedene Systeme so gekoppelt werden, dass wichtige Ereignisse und Ansteuerungen auf beide Systeme wirken.

Besucherverwaltung

Die Verwaltung von Besuchern unterscheidet sich von derjenigen der Mitarbeiter durch die meist zeitlich begrenzten Rechte, die Sperrung des Ausweises nach der Rückgabe und Wiederverwendung für den nächsten Besucher usw. Dennoch ist die Nachvollziehbarkeit gegeben.

Funktionalitäten und Vorteile:

// Zugang möglich, auch wenn der Empfang nicht besetzt ist (Selbstregistrierung)
// Voranmeldung von Besuchern und automatische Begrüssung
// Besucher können sich innerhalb von vordefinierten Zonen frei bewegen
// Protokollierung der Zutritte ist jederzeit sicher gestellt
// Archivierung aller Besuche inkl. besuchte Person
// Übersicht der sich im Gebäude befindlichen Besucher (Notfall, Evakuation)
// Identifikation von unerwünschten Personen und Firmen (Blacklist)
// Zusatzfunktionen wie Raum- und Ressourcenreservation (z.B. Catering)
// Geregelter Zutritt in heikle Zonen (verhindert, begleitet usw.)
// Freischaltung von Liften für gewisse Etagen
// Parkplatz-Management

Integration in Sicherheits-/Gebäudeleitsystem

Die Einbindung der Zutrittskontrolle in ein Sicherheitsleitsystem (SLS) ist weit verbreitet , erlaubt diese doch dem Sicherheitspersonal eine einheitliche und gemeinsame Bedienung aller Sicherheits-Subsysteme und einen Gesamtüberblick. Die Bedienung erfolgt über eine übersichtliche grafische Oberfläche.

Folgende Zustände können bei der Visualisierung der Türen sinnvoll sein:

// Türe zu (Magnetkontakt im Türfalz)
// Türe geschlossen bzw. verriegelt (Kontakte im Schliessblech oder im Schloss)
// Türe zu lange offen (Vorwarn-Summer vor Ort, damit die Türe rechtzeitig geschlossen wird)
// Türalarm (ohne berechtigte Lesung geöffnet oder zu lange offen)

Folgende Aktionen können beispielsweise ab einem Leitsystem vorgenommen werden:

// Einmalige Fernöffnung von Türen und Toren
// Öffnung/Schliessung für eine bestimmte Zeit
// Daueröffnung
// Dauersperre

Alarmweiterleitung

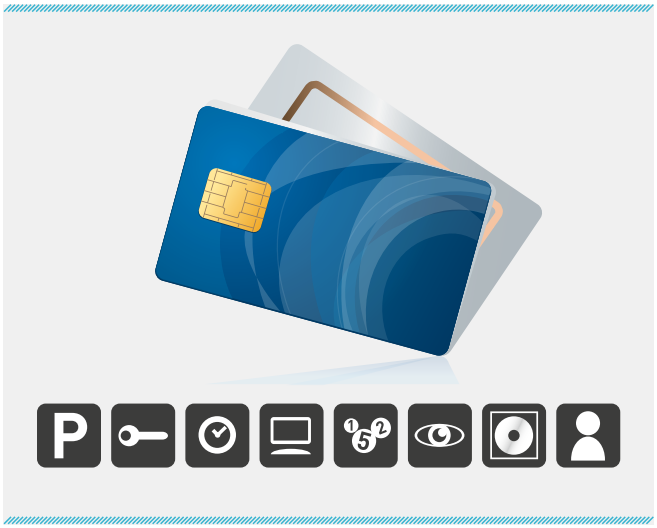
Eine Alarmweiterleitung an die Polizei oder private Interventionsstellen, z.B. per SMS oder E-Mail, sollte gesichert/verschlüsselt erfolgen. Eine interne Benachrichtigung, z.B. des technischen Leiters, kann einen Zusatznutzen schaffen. Häufig wird die Zutrittskontrolle als Bedienelement der Einbruchmeldeanlage (EMA) genutzt. Je nach Möglichkeit des Zutrittssystems ergeben sich aus dieser Kombination komfortable Lösungen. Abläufe können automatisiert und Synergien genutzt werden. Wichtig: Die Zutrittskontrolle ersetzt die EMA nicht. Die Komfortlösungen im Zusammenhang mit der Zutrittskontrolle können nicht SES-zertifiziert werden.

Videoüberwachung

Eine Anbindung an ein Videoüberwachungssystem kann Sinn machen. Aufnahmen von erlaubten und nicht erlaubten Zutritten erleichtern die nachträgliche Feststellung eines allfälligen Ausweismissbrauchs. Die entsprechenden Programme ermöglichen die sofortige Aufschaltung der Videokamera via Bewegungsmelder, sobald sich jemand der Zufahrt oder Tür nähert oder an einem Leser eine Buchung macht. Dies erlaubt dem Sicherheitspersonal eine zusätzliche Kontrolle, entweder live am Bildschirm oder nachträglich aufgrund der gespeicherten Bilddaten.

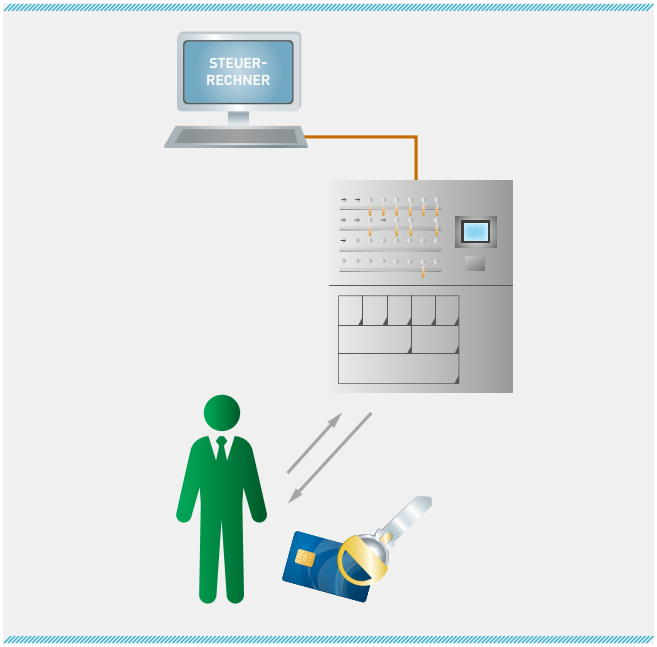
Ausweiserstellung und -verwaltung

Viele Zutrittskontrollsysteme verfügen nebst der Ausweisverwaltung über Module für die Personalisierung des Ausweises, wie z.B das Bedrucken und Programmieren. Im Rahmen der Ausweisverwaltung sind nebst dem eigentlichen Zutritt auch Anwendungen wie die Parkplatzverwaltung, bargeldloses Bezahlen, Kopiererbenutzung, Schlüsseldepot, Leihgabenverwaltung usw. möglich. Nur spezialisierte Anbieter von Zutrittskontrollsystemen bieten solche Module an.



Schlüsseldepot

Durch den Einsatz eines elektronischen Schlüsseldepots verlassen keine Schlüssel mehr das Firmenareal.



Die Vorteile eines Schlüsseldepots in Kombination mit einer Zutrittskontrolle sind vielfältig:

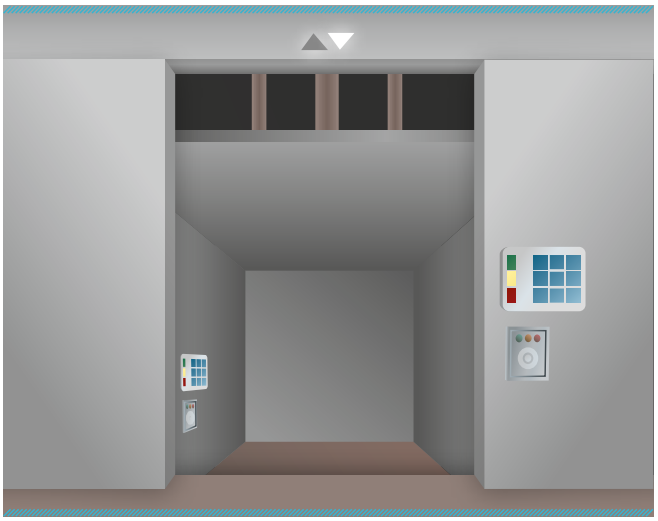
// Jede Schlüsselentnahme und –rückgabe wird automatisch protokolliert: wer, wann, welcher Schlüssel?
// Klare Vergabe von Rechten (wer darf wann welchen Schlüssel beziehen?)
// Überwachung der entnommenen Schlüssel (welche Schlüssel fehlen gerade jetzt?)
// Alarmierung bei nicht erfolgter Rückgabe zu einem bestimmten Zeitpunkt, beziehungsweise kein Austritt aus dem Gebäude, solange ein Schlüssel nicht deponiert ist
// Weniger Schlüssel im Umlauf

Ein Depot kann sich auch für andere Dinge eignen, wie z.B. Werkzeuge, Arbeitsmittel (PCs) usw.

Liftsteuerung

Varianten für die Kombination von Zutrittskontrolle und Liftsteuerung:

// Der Lift kann nur von berechtigten Personen gerufen werden. Die Zutrittsleser befinden sich nicht in der Kabine, sondern auf den Etagen und dienen zum Rufen des Lifts.
// Der Zutrittsleser befindet sich in der Kabine:
/ Alle Stockwerke sind nach einer gültigen Buchung frei wählbar.
/ Nach einer Buchung wird das dem Medium zugewiesene Stockwerk angefahren.
/ Es können nur Stockwerke gewählt werden, für die eine Berechtigung vorliegt (Freischaltung der Tasten).



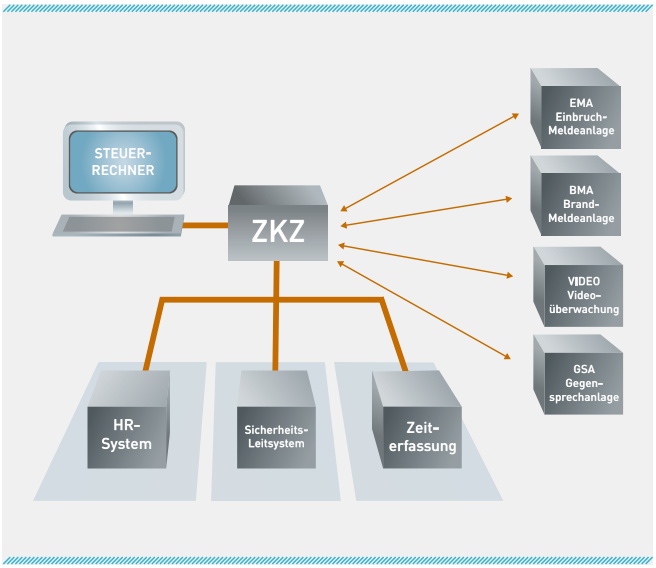
Bei Liftsteuerung zu beachten:

Je früher die Möglichkeiten des Lift- und Zutrittskontrollliefe-ranten koordiniert werden, desto besser. Achtung: Ein Lift ist keine Personenvereinzelung.

Schnittstellen zu Drittsystemen

Eine Anbindung über serielle Schnittstellen kann z.B. für die Integration von Biometrie-Systemen, Liftsteuerungen oder auch von Videoüberwachungsanlagen verwendet werden.

Auf Managementebene kann ein Datenaustausch über das Netzwerk erfolgen, was für die Übernahme von Personaldaten von einem HR-System üblich ist und die redundante Datenerfassung eliminiert. Neben der Vereinfachung und der Fehlervermeidung erhöht dies auch die Sicherheit, werden doch im HR-System Ein- und Austritt sowie Abteilungswechsel zuverlässig gepflegt.



Schnittstellen können je nach Anforderung (Art der Daten, Periodizität, Zugriffsverfahren, Verfahren bei Fehlern und Konflikten, Protokollierung usw.) und Implementierung sehr aufwendig sein. Es braucht viel Erfahrung und Kenntnisse der beiden zu koppelnden Systeme.

Zutrittskontrolle und Zeiterfassung

Gemeinsame Elemente beider Systeme sind der Ausweis (Identifikation) und die Stammdaten (Personendaten).

Daher gibt es verschiedene Systeme, die neben der Zutrittskontrolle auch eine integrierte Zeiterfassung und -verar-

beitung bieten. Der Vorteil einer integrierten Lösung: Der Zugang zum Gebäude ist z.B. nur möglich, wenn er zum richtigen Zeitpunkt erfolgt, d.h. z.B. während der entsprechenden Schicht, nicht aber während der Ferien.

Ob eine integrierte Lösung oder nur die Koppelung über eine Schnittstelle die bessere Lösung ist, muss individuell und anhand der Anforderungen des Nutzers beurteilt werden. Einige Fragen, die zu klären sind:

- Kann das Personalinformationssystem Daten zur Verfügung stellen?
- Welche Kartentechnologie soll verwendet werden?
- Wie sind die Verantwortlichkeiten (Betrieb, Unterhalt usw.) geregelt?
- Welche Anforderungen werden an die Zutrittskontrolle gestellt?
- Welche Anforderungen werden an die Zeiterfassung bzw. -verarbeitung gestellt?
- Gibt es Anforderungen seitens Lohn- und HR-Systeme?
- Welche Datenbank-Technologie ist im Einsatz?
- Gibt es weitere Verknüpfungen mit der Betriebsdaten- bzw. Leistungserfassung?

Zutrittskontrolle und Einbruchmeldeanlage

Die Koppelung von EMA-Systemen erfolgt hauptsächlich über Kontakte (I/O's), die normalerweise einfach zu handhaben sind. Dennoch kommt es vor allem bei Türen, die durch ein EMA-System überwacht werden, immer wieder zu ungewollten Alarmen, weil ZuKo und EMA nicht korrekt miteinander kommunizieren. Deshalb empfiehlt sich für EMA-überwachte Türen eine sorgfältige Planung.

Lokale Applikation vs. Web-Client

Die meisten ZuKo-Systeme ermöglichen die Datenhaltung und Kommunikation mit den Peripheriegeräten mittels eines Servers. Die Erfassung und Bewirtschaftung von Zutrittsdaten erfolgt entweder über «normale» Clients oder über Web-Clients, zwei Philosophien mit Vor- und Nachteilen.

Bei einer Installation mit Clients wird auf jedem relevanten PC eine Software installiert, die auf die Daten des Servers zugreift. Diese Technologie ermöglicht eine gute und schnelle Bedienung der Zutrittskontrolle sowie eine sichere und performante Steuerung der Systeme. Ein Update der Applikation muss aber an jedem PC erfolgen und ist entsprechend aufwendig.

Bei der Web-Client-Lösung ist auf dem Zutrittskontroll-Server eine Web-Applikation installiert, welche den Zugriff via Internetbrowser ermöglicht (z.B. Internet Explorer, Chrome oder Mozilla Firefox). Diese Lösung hat den Vorteil, dass auf den einzelnen Arbeitsplätzen keine separate Software mehr installiert werden muss. Jeder Arbeitsplatz im Netzwerk wird dadurch zu einem Zutrittskontroll-Arbeitsplatz. Während für das einwandfreie Funktionieren der Webinstallation die Internet-Bandbreite heute kein Thema mehr ist, müssen trotzdem einige Parameter richtig eingestellt sein. Ein Update erfolgt nur noch auf dem Server.

Workflow (Antragssystem)

Mehrstufige Antragsverfahren für Zutrittsberechtigungen erfolgen nicht mehr mittels Formularen, sondern mittels Softwarekomponenten, welche in einen automatisierten Workflow intergriert sind. Sie steuern Antrags-, Vergabe-, Mutations- und Kontrollprozesse.

Identity and Access Management (IAM)

Softwarelösung zur Verwaltung von Identitäten, Berechtigungen und Medien. Ziel des IAM ist es, den richtigen Personen zum richtigen Zeitpunkt die richtigen Zutritts- und Zugriffsrechte zu erteilen. Letztere sind abhängig von Funktionen, Aufgaben und Geschäftsprozessen.

Reporting

Ein Zutrittssystem muss die Möglichkeit bieten, Berichte und Auswertungen zu erstellen. Nebst vordefinierten Abfragen sollten vielfältige, nach unterschiedlichen Kriterien gefilterte Abfragen sowie deren Export in gängige Office-Programme möglich sein. Je spezieller die Anforderungen, desto mehr lohnt sich die genaue Spezifikation solcher Reports und die Prüfung des dafür nötigen Aufwandes.

KEIN ZUTRITT OHNE ZULASSUNG

Die meisten Produkte müssen durch ein anerkanntes Prüflabor im Auftrag des Herstellers bzw. der Vertriebsgesellschaft getestet werden. Sind die Anforderungen erfüllt, bestätigt das Labor die Konformität zur Norm in einem Prüfbericht. Die Zulassungsstellen im entsprechenden Land erteilen aufgrund der Prüfberichte die entsprechende Zulassung/Anerkennung für die Produkte und Systeme.

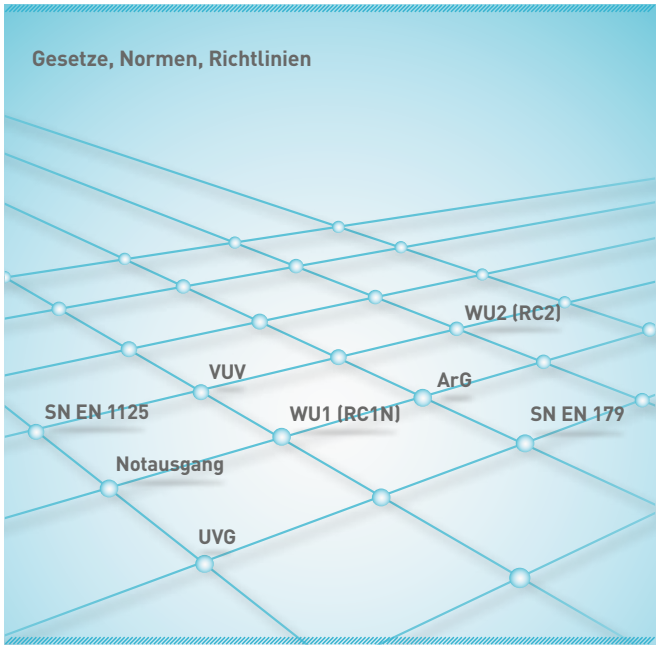
Folgende Schweizer Institutionen spielen für die Zulassung von Produkten und Systemen sowie die Definition von Vorgaben und Normen eine Rolle:

	Prüfinstitut	Zertifizierung, Zulassung, Anerkennung	Normen, Definition	Richtlinien, Vorschriften
Electrosuisse, ehemals SEV Verband für Elektro-, Energie und Informationstechnik	(CH)	(CH)	(CH)	
SES Verband Schweizerischer Errichter von Sicherheitsanlagen				CH
SNV Schweizerische Normen-Vereinigung			CH	
SQS Schweizerische Vereinigung für Qualitäts- und Management Systeme		CH		
SVV Schweizerischer Versicherungsverband		(CH)		

Der im Jahre 1972 gegründete Verband Schweizerischer Errichter von Sicherheitsanlagen SES bezweckt die generelle Förderung des Schutzes von Menschen und Werten mit technischen Systemen. Ereignisse sollen frühzeitig erkannt und damit Schäden verhütet werden. Ein besonderes Anliegen ist die Anerkennung der Systeme durch relevante Aufsichtsbehörden und Versicherungen.

Bauliche Vorgaben und Normen

Die baulichen Vorgaben stützen sich auf Gesetze und Normen betreffend Brandschutz, Einbruchschutz, Fluchtwege, Intervention, usw. Zum Teil ist es nicht zulässig, Produkte beliebig zu kombinieren. Bei Brandschutztüren muss die Kombination von verschiedenen Systemen zertifiziert sein. Es ist beispielsweise nicht zulässig, Elemente (z.B. Schloss, Türblatt) im Nachhinein zu ändern.



SOVIEL WIE NÖTIG, SO WENIG WIE MÖGLICH

Grundlage für die Erstellung und Bewirtschaftung einer Personendaten-Sammlung bildet das Bundesgesetz über den Datenschutz DSG. Dieses regelt, wer unter welchen Bedingungen Daten beschaffen, aufbewahren, bearbeiten, verwenden und veröffentlichen darf und welche Rechte diejenigen Personen haben, über welche Daten angelegt werden.

Die Beschaffung von Personendaten muss für die betroffene Person transparent sein.

Bei der Bearbeitung von besonders schützenswerten Personendaten ist die Einwilligung der Betroffenen ausdrücklich erforderlich. Als besonders schützenswert gelten Daten über:

// Religiöse und politische Ansichten oder Tätigkeiten
// Rassenzugehörigkeit
// Gesundheit und Intimsphäre
// Strafrechtliche Tatbestände
// Sozialhilfe

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugten Zugriff geschützt werden.

Umgang mit Daten aus der Zutrittskontrolle

Die Zutrittskontrolle muss dafür geeignet sein, den Schutz von Personen und/oder Sachen zu gewährleisten. Sie darf nur zum Einsatz kommen, wenn die Verhältnismässigkeit gegeben und andere, die Privatsphäre weniger beeinträchtigenden Massnahmen ungenügend oder undurchführbar sind.

Die Datensammlung und -bearbeitung muss zweckgebunden sein und auf das absolut erforderliche Mass reduziert bleiben. Aus den Daten dürfen sich keine weiteren Angaben zur betroffenen Person, insbesondere über ihren Gesundheitszustand, ihre Religionszugehörigkeit usw. ableiten lassen.

Die Daten, insbesondere diejenigen, die Rückschlüsse auf das Verhalten einer Person erlauben, dürfen nur so lange gespeichert werden, wie dies der Zweck unbedingt erfordert. Der Zugriff auf die Daten muss zudem auf den minimalen, relevanten Personenkreis beschränkt bleiben. Die Daten dürfen nicht weitergegeben werden, ausser zur Anzeigenerstattung an die Strafverfolgungsbehörden. Jeder Zugriff und jede Bearbeitung muss lückenlos und revisionssicher protokolliert werden.

PLANUNG, PLANUNG UND NOCHMALS PLANUNG

Projektleiter

In der Verkaufsphase ist es meist nicht möglich oder sinnvoll, sämtliche Parameter so detailliert zu klären, dass das ZuKo-System alle Anforderungen des Kunden präzise erfüllt. Hier kommt der Projektleiter ins Spiel.

Aus der Abwicklung von unzähligen Projekten und der gesammelten Erfahrung ist die nachfolgende Fragenliste entstanden, die gleichzeitig die Komplexität solcher Projekte aufzeigt und die Vielfalt an Themen, mit denen Auftraggeber wie auch Auftragnehmer konfrontiert werden. Sie erhebt gewiss nicht den Anspruch auf Vollständigkeit.

Projekt allgemein

// Wann muss das Projekt als gesamtes abgeschlossen und dem Kunden übergeben sein?
// Bis wann sind welche baulichen Einrichtungen gemacht (Wände, Türen, Lifte, Tore, usw.)?
// Welche visuellen Anforderungen (Design, Unterputzmontage usw.) werden an die Installation gestellt?
// Wer entscheidet bei technischen Projektänderungen und -erweiterungen?
// Wer entscheidet bei organisatorischen Projekt- und betrieblichen Prozessänderungen?
// Wer entscheidet über Budgeterhöhungen und wie müssen Nachträge offeriert, bestellt, beauftragt, überwacht und abgewickelt werden?

Ausgangslage und Organisatorisches

// Hat der Kunde bereits ein Zutrittssystem, das es abzulösen gilt?
// Wie kann der Betrieb während der Ablösung sichergestellt werden?
// Welche Bereich sind wie zu schützen?
// Welche Bereiche müssen geregelt betreten werden können?
// Wer ist für die Betreuung der Systeme verantwortlich?
// Wer vergibt die Berechtigungen?
// Wer verwaltet die Daten im System?
// Gibt es mehrere Kunden, welche das System nutzen? Werden separate Mandanten benötigt?
// Wie viele Mitarbeiter, Besucher, Lieferanten müssen mit einem Medium ausgerüstet werden?
// Muss eine Besucherverwaltung mit Berechtigungen auf Ausweisen möglich sein?

// Wie und wo sollen die Medien produziert, programmiert, personalisiert und ausgegeben werden?
// Wer darf an welchen Systemen, Modulen usw. was sehen, erstellen, editieren und löschen können?
// Wer hat in welchen Bereichen welche Rechte für den Zutritt?
// Wer hat welche Rechte für welche Personen(kreise)?
// Wer hat welche Rechte für welche Unternehmensbereiche, z.B. Mandanten?

IT-Architektur

// Welche Leitungsnetze dürfen, sollen oder müssen verwendet werden?
// Wie sehen die IT-Architektur und deren Security-Policy aus?
// Wer ist für die Einbindung in die IT-Landschaft verantwortlich?
// Wann und wie kann eine Verbindung, Einbindung, Anbindung usw. in die IT-Umgebung erfolgen?
// Wer ist für IP-Adressen, Switch-Aufschaltungen (Patchungen), Firewall-Themen usw. zuständig? Bei wem und wie muss was beantragt werden?
// Welche Systeme dürfen, sollen oder müssen von wo gespiesen werden?
// Welche Systeme dürfen, sollen oder müssen an Notstromversorgungen angeschlossen werden?
// Wer bestellt, organisiert und installiert die Strom- und Notstromversorgungen (USV)?

Datenhandling

// Müssen Daten einmalig vom heutigen System oder Drittsystem übernommen werden?
// Welche Daten (z.B. Personaldaten) werden wie und in welchen Intervallen aus welchem System in die Zutrittskontrolle übernommen?
// Welche Daten (z.B. Bewegungsdaten, Buchungen, Alarmmeldungen) werden wie und wie oft an welche Drittsysteme übergeben?
// Wie sollten die Daten gespeichert, gehalten und gesichert werden?
// Welche Datenbanktechnologien dürfen, sollen oder müssen verwendet werden?

Bedienung und Medien

// Welche Lesemethode wird gewünscht (handfrei, mit oder ohne Medium usw.)?
// Wenn mit Medium, mit welchem (Schlüssel, Ausweis, Biometrie usw.)?
// Werden auch Lifte und Stockwerke selektiv gesteuert?
// Werden Schnittstellen zu EMA, BMA, GSA und Videoüberwachung benötigt und wenn ja, welche?
// Welche Applikationen sollen mit dem Berechtigungsmedium (z.B. Ausweis) betrieben werden?
// Dient das Medium auch als Mitarbeiterausweis?
// Was ist deren Speicherbedarf resp. welches sind die Anforderungen an die RFID-Technologie?
// Wer erstellt den Ausweis (Druck/Personalisierung) erstinstanzlich und im Betrieb?
// Welche integralen oder angebundenen Zusatzanwendungen (Parkplatzverwaltung, Ausweiserstellung, Visualisierung auf dem Monitor, Besucherverwaltung, Besucher-voranmeldung usw.) sind vorgesehen?
// Müssen sofortige Sperrungen oder Freigaben an entsprechenden Türen möglich sein?

Bauliche Normen

// Welche Massnahmen für den Brandschutz, Einbruchschutz sind zu treffen?
// Wo sind die Fluchtwege, wo können Interventionen stattfinden?
// Sind die Brandschutztüren zertifiziert?

Reporting

// Welche Informationen müssen wann, wo und wie aus dem System verfügbar sein?
// Muss jederzeit eine Echtzeit-Protokollierung aller Bewegungen möglich sein?

UND WIE HÄTTEN SIE ES DENN GERNE?

Das Zutrittssystem kann ohne Mitwirkung des Kunden nicht realisiert werden! Der Projektfortschritt und die Termineinhaltung können nur gewährleistet werden, wenn auch auf Kundenseite die erforderliche Zeit zur Verfügung steht.

Der Kunde muss u.a. das Rechtekonzept definieren. Es soll auf Anhieb flexibel genug und auf Nutzergruppen (Mitarbeiter, Besucher, Lieferanten, Temporäre u.a.) ausgerichtet sein. Kleine Anpassungen sind zwar immer möglich, die Erarbeitung eines komplett neuen Konzeptes bedeutet aber meistens: Zurück zu Feld 1.

Tipp: Ein Projektleiter auf Kundenseite ist für die erfolgreiche Umsetzung des Projekts entscheidend.

Projektverantwortlichkeiten

Die Aufgaben und Verantwortlichkeiten müssen klar definiert sein. Dazu hilft meistens eine einfache Skizze mit der Projektorganisation.

Einige mögliche Aufgaben in einem Projektteam:

// Projektleiter
// Auftraggeber (bei Kosten, Nachträgen, usw.)
// Systembetreiber
// Systembenutzer/-bediener
// IT-Leiter (IT-Policy)

Weitere wichtige Rollen ausserhalb des Projektteams:

// Elektroplaner, Elektriker
// Türkoordinator, Türbauer, Torbauer, Schloss- und Beschlagslieferant, Zylinderlieferant
// Schreiner, Schlosser, Maurer, Maler
// Bauleiter, Architekt, Innenarchitekt
// Behörden (z.B. Verband Kantonaler Feuerversicherungen VKF betreffend Brandschutz und Fluchtwege)

Beim Lieferanten sollten mindestens folgende Rollen bestimmt sein:

// Projektleiter
// Systemtechniker Hardware
// Systemtechniker Software
// Verkaufsberatung (Auftragsverhandlung, Pflichtenheft, Nachträge)
// Projektadministrator (Finanz-Controlling)

Anspruchsgruppen und ihre Bedürfnisse

Verschiedene Anspruchsgruppen – teilweise deckungsgleich mit den Projektteilnehmern – haben auch verschiedene Bedürfnisse, die bekannt sein und, wo erforderlich, auch berücksichtigt werden sollten.

Systembediener: Einfaches, logisches System; einfache, intuitive Bedienung; hohe Verfügbarkeit; Informationen bei Bedarf vollständig und sofort verfügbar; guter Support (Bedienerunterstützung), höchste Zuverlässigkeit

Auftraggeber: Tiefe Initialkosten; Investitionsschutz; tiefe Betriebskosten während der gesamten Betriebsdauer und lange Nutzung des Systems

Mitarbeiter: Komfort; Türe muss von selber aufgehen; Funktion muss immer gewährleistet sein; Zutritt «ohne» Hindernisse

Architekt: Design; muss sich in die Architektur einfügen und so unauffällig wie möglich sein; kein planerischer Aufwand

IT-Leiter: Sicherheit; keine Verletzung der Policy; Nutzung der bekannten IT-Infrastruktur (Hardware, Datenbanken, Netzwerk usw.); möglichst keine nötige Erweiterung des Mitarbeiter-Know-hows

Weitere Anspruchsgruppen

// Antragsteller von Zutrittsrechten
// Erteilen von Zutrittsrechten
// Umsetzer von Zutrittsrechten (Zutrittsadministration)
// Fremdfirmen (u.a. Besucher)
// Sicherheitsorganisation
// Gesamtorganisation
// Mieter (Gewerbepark)
// Personalwesen
// Facility-Management
// Lieferanten und Dienstleister (z.B. Provider)
// Staat, Gesetzgeber, Revisionsstellen

Einbezug ins Projekt

Es ist empfehlenswert, wenn nicht sogar elementar, dass die internen Strukturen, betrieblichen Abläufe, Angewohnheiten der Mitarbeiter (und vor allem der Entscheider) bei der Umsetzung eines ZuKo-Systems berücksichtigt werden. Andernfalls können schnell Vorbehalte gegenüber dem System aufkommen, welche die Projektierung und Abläufe behindern. Daher ist es wichtig, Personen aus den verschiedenen Abteilungen in den Prozess einzubeziehen, deren Bedürfnisse und Bedenken abzuholen und diese als Botschafter für die Lösung zu gewinnen.

Anforderungen an die IT

Ein Zutrittskontrollsystem kann in heute üblichen IT-Umgebungen betrieben werden, solange die Anforderungen des Kunden erfüllt werden. Sind Zutrittssystem und Kunden-IT nicht kompatibel, muss entweder ein darauf aufbauendes System oder eine eigene Umgebung geschaffen werden.

Folgende Punkte sind zu klären:

// Kann das IT-Netz des Kunden verwendet werden?
// Wenn nein, wer soll das benötigte Netzwerk erstellen und zukünftig betreuen?
// Wer liefert Server, Clients, Peripheriegeräte, Medien, usw.?
// Wer liefert die Betriebssysteme und welche?
// Wer liefert und pflegt die Datenbank und welche?
// Wer liefert allfällige Web-Server und welche?
// Wer ist für die Netzwerk-Administration zuständig?
// Wer ist für die Domain-Verwaltung (URL-Adressen) zuständig?
// Wer ist für die Benutzerrechte, Passwortvergabe, Firewall, IP-Adressen, usw. zuständig?
// Wie und wo dürfen, sollen oder müssen Daten gespeichert und gesichert werden?

EIN HANDBUCH FÜR DIE VIELEN HÄNDE

Etappierung

Es empfiehlt sich, Projekte mit einer gewissen Komplexität in Etappen zu organisieren und abzurechnen. Eine solche Staffelung zwingt Betreiber (Kunde) und Lieferant zu einer klaren, logischen Strukturierung der Teilprojekte, bringt Transparenz bezüglich der Projektlaufzeit und eine Fortschritts- und Kostenkontrolle. Entscheide, Termine und Verantwortlichkeiten sollten in Sitzungsprotokollen festgehalten werden.

Dokumentation

Zu einem Zutrittskontrollsystem gehört eine saubere Dokumentation, welche dem Benutzer, dem Betreiber und dem Lieferanten eine klare Übersicht über die installierten Komponenten und die Software gibt. Das Betriebskonzept dokumentiert die Funktionen der Zutrittskontrolle, erklärt die Systemkomponenten und ihre Aufgaben und Schnittstellen. Die Dokumentation soll es jederzeit ermöglichen, dass ein Projekt auch von einer Person weitergeführt werden kann, die bisher noch nicht beteiligt war.

Auch der Datenschutz, die Datensicherung sowie die Zuständigkeiten sollten in einem Konzept dokumentiert und geregelt sein.

AUCH DAS SCHUTZSYSTEM BRAUCHT SCHUTZ

Das Zutrittssystem soll so geschützt sein, dass die Sicherheit nicht durch einfache organisatorische oder technische Massnahmen gefährdet wird oder das System durch einen Angriff nicht mehr zur Verfügung steht. Dazu bedarf es eines strukturierten Schutzkonzeptes. Man bedenke: ca. 70 % der Computerkriminalität wird von eigenen Mitarbeitern begangen.

Neben dem System sind die Personendaten besonders zu schützen. Das Datenschutzgesetz DSG verlangt, Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugten Zugriff zu schützen.

Sicherheit kann dem Komfort zuwiderlaufen. Schränkt das System einen Mitarbeiter zu stark ein oder sind ihm die Gründe für die Einschränkungen nicht klar, wird er Mittel und Wege finden, diese zu umgehen.

Teilaspekte des Sicherheitskonzeptes:

// Verfügbarkeit – Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden. Die Verfügbarkeit ist hoch, wenn möglichst keine Defekte und Fehlbedienungen vorkommen, was u.a. durch die richtige Wahl der IT-, Netzwerk- und Türkomponenten sowie Service und Schulung sichergestellt werden kann.

// Hardware – Ausweiskarte, Leser, Türkomponenten, Kontroller, Clients usw. müssen vor Zugriff, Sabotage, Viren, Vervielfältigung und ähnlichem geschützt sein.

// Informationssicherheit – Informationsverarbeitende und -lagernde Systeme müssen die Vertraulichkeit, Verfügbarkeit und Integrität von Daten sicherstellen. Dies kann z.B. durch Verschlüsselung erfolgen.

// Verbindlichkeit – Sämtliche Ereignisdaten (Zutritt, Türöffnung usw.) müssen vollständig und chronologisch protokolliert sein und einer Revision standhalten.

ZUVERLÄSSIGKEIT ERHÖHEN, LEBENSDAUER VERLÄNGERN

Das Funktionieren der Zutrittskontrolle und somit die Sicherheit von Menschen und Gebäuden sind nur mit einem intakten System gewährleistet. Dazu braucht es den professionellen und gewissenhaften Service und Unterhalt von Soft- und Hardware, aber auch eine leistungsfähige Serviceorganisation.

Schnittstellen

Bei Projekten und Systemen mit der Komplexität von Zutrittskontrollen müssen verschiedene Leistungserbringer optimal zusammen arbeiten. Nicht nur bei Planung und Ausführung, sondern auch bei Störungen sind die Beteiligten und Zuständigkeiten klar zu regeln: Wo ist das Problem aufgetaucht? Wer muss es beheben?

Die Partei, welche im Ereignisfall für das Aufgebot der Lieferanten zuständig ist, sollte dabei ein gutes Gesamtverständnis des Systems und der Zusammenhänge mitbringen. Bei der Definition der Schnittstelle sind Lücken, aber auch Überlappungen zu vermeiden. Lässt sich z.B. eine Türe nicht begehen, wird zuerst der Lieferant des Zutrittssystems aufgeboten. Der Kunde/Betreiber hat nicht bemerkt, dass eine leichte Deformation der Türe (Temperatur) vorliegt und folglich wegen eines defekten Kontaktes keine Informationen mehr ans System übermittelt werden. Anstatt nur der Türbauer werden beide Lieferanten aufgeboten – mit entsprechenden Kostenfolgen.

Aufgabenteilung

Lieferanten und Kunde oder ein beauftragter Provider (Facility Manager, Haustechnik, IT) können sich den Betrieb und Unterhalt des Zutrittskontrollsystems auch teilen. Nachfolgend einige Leistungen, die in einem Wartungsvertrag enthalten und geregelt sein können:

- Bereitschaft: Serviceorganisation, Stammdatenpflege, Ersatzteile usw.
- Instandhaltung/präventive Wartung: Fehlerdiagnose, Systemstabilität, Updates usw.
- Instandsetzung: Störungsbehebung, Überprüfung nach Interventionen
- Datensicherung/Datenwiederherstellung
- Software: Patches, Updates, Upgrades, Beratung
- Bevorratung und Lieferung von Ersatzteilen
- Netzwerk-Support
- PC-/Server-Support
- IT-Security
- Schulung
- Alarm Management
- Pikettdienst
- Fixtime: Garantierte maximale Standzeit kritischer Anlageteile

Das Leistungsverzeichnis des SES listet die Komponenten, die gewartet werden sollten und in welcher Periodizität.

Service Level Agreement SLA (Wartungsvertrag)

Ein Wartungsvertrag macht Kosten kalkulierbar. Fallen hohe Reparaturkosten an (Arbeit und Material), sind diese durch den Vertrag gedeckt.

Die regelmässige Wartung der Anlage erhöht dessen Verfügbarkeit und Nutzungsdauer. Der Lieferant sollte in der Lage sein, an 365 Tagen rund um die Uhr eine Instandsetzung vorzunehmen, falls der Kunde dies braucht und im Werkvertrag so geregelt haben will. Soll eine Intervention auch ausserhalb der Arbeitszeit sichergestellt sein, kann dies meist nur über einen Wartungsvertrag vereinbart werden.

Betreiber sollten sich von ihren Lieferanten ausführlich beraten lassen, die einzelnen Module eines Vertrages erfragen und dann entscheiden, welche Leistungen ihnen wichtig sind. Es macht durchaus Sinn, bereits während der Gewährleistungszeit einen Wartungsvertrag abzuschliessen.

Schulung

Schulungen von Zutrittskontrollsystemen beschränken sich meistens auf die Applikation, die Einrichtungs- und Bedienungsfunktionen sowie die täglichen Aktionen. Bei diesen Schulungen sollten stets Bedienungshandbücher (ev. in elektronischer Form) abgegeben werden. Die Schulung sollte unter Verwendung dieser Unterlagen erfolgen, dienen sie doch als Nachschlagewerk. Falls die Kunden/Betreiber oder das Facility Management gewisse Instandsetzungen selber vornehmen, ist auch hier eine periodische Schulung angezeigt.

SES – DIE QUALITÄTSMARKE DER SICHERHEITSTECHNIK

Der Verband Schweizerischer Errichter von Sicherheitsanlagen SES umfasst die in dieser Branche führenden Unternehmen in der Schweiz.

SES-Mitglieder gehören zu den Fachfirmen, welche vom Schweizerischen Versicherungsverband SVV und/oder von der Vereinigung Kantonaler Feuerversicherungen VKF anerkannt sind. Zudem sind in der Sektion Security auch bewährte Errichter von Zutrittskontroll- (auch Access Control oder AC) und Videoüberwachungssystemen (CCTV) vertreten.

Tätigkeiten

Der SES legt unter anderem die Qualitätsrichtlinien fest, normiert Geräte, bewertet Alarm- und Löschanlagen und arbeitet mit Behörden, Polizei, Feuerwehr, Versicherungen und Telekommunikationsfirmen zusammen, um den Bau und die Prüfung von Sicherheitsanlagen auf höchstem Niveau zu gewährleisten.

Nur ein Ziel: Seriosität

Mit dem Q-Label bestätigt die SES-Fachfirma, vielfältige Qualitätskriterien sowie Sicherheitsnormen und Richtlinien einzuhalten. Als SES-Mitglied gewährleistet sie ihren Kunden durchdachte, dauerhafte Sicherheitslösungen und verpflichten sich,

- // mindestens drei Jahre Erfahrung im Errichten von AC-Anlagen zu haben,
- // nur Geräte zu installieren, die von den zuständigen Stellen anerkannt sind,
- // für die Projektierung, Installation, Inbetriebnahme und Wartung ausnahmslos gut ausgebildetes Personal einzusetzen, das regelmässig Weiterbildungen besucht,
- // die Installation von Anlagen nach dem neuesten Stand der Technik vorzunehmen,
- // einen Störungs- und Wartungsdienst zu gewährleisten,
- // ein eigenes Ersatzteillager zu führen, um bei Bedarf rasch intervenieren zu können.

Sind diese und weitere Bedingungen erfüllt, darf der betreffende Anbieter dieses Label verwenden.

Verband Schweizerischer Errichter von Sicherheitsanlagen SES

Technische Arbeitskommission, Untergruppe Access Control (AC)

Mitglieder

Simon Amberg
Tyco Fire and Integrated Solutions AG
Produktmanager

Guido Salerno (Gruppenleitung)
Securiton AG
Fachstelle Zutritts- und Zeiterfassungssysteme

Roland Hunkeler
Siemens Schweiz AG
Produktmanager

Roger Schurtenberger
KABA AG
Verkaufsleiter

Max Keller
Siaxma AG
Geschäftsführer

Viktor Zeltner
Bixi Systems AG
Produktmanager

Schweizerischer Verband der Errichter von Sicherheitsanlagen SES
Alpenstrasse 20 | 3052 Zollikofen | T +41 31 910 15 45 | info@sicher-ses.ch | www.sicher-ses.ch