Zutrittssteuerung

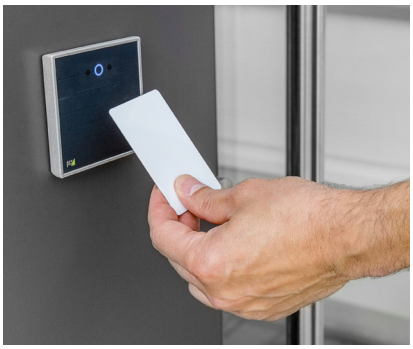
Informationen für Anwender und Sicherheitsbeauftragte

Systeme zur Zutrittssteuerung – meist noch als Zutrittskontrolle, aber auch als Zutrittssysteme bezeichnet - haben die Aufgabe, die Wahrscheinlichkeit eines Verlustes im personellen, materiellen oder immateriellen Bereich zu verringern. Berechtigte Mitarbeiter eines Unternehmens sollen durch einfache und schnelle Identifikation Zutritt erhalten. Das Betreten von Räumen, Gebäuden und Arealen durch Unbefugte wird verhindert, während berechtigte Personen einen reibungslosen Zutritt haben.

Die Zutrittssteuerung dient u. a. dem Schutz vor Diebstahl, Sabotage sowie Übergriffen auf Mitarbeiter. Auch Industriespionage, die in den letzten Jahren in Deutschland und Westeuropa erhebliche Schäden verursacht hat, kann mittels Zutrittssteuerung verhindert werden. Deshalb sind Zutrittssysteme vornehmlich in wirtschaftlich genutzten Einrichtungen wie Unternehmen, Verwaltungen, Hotels, Kraftwerken, Flughäfen und Veranstaltungsorten zu finden.

1. Aufgaben der Zutrittssteuerung

Zutrittssysteme steuern die Zutritts- und Zufahrtsberechtigung von Personen und Fahrzeugen zu festgelegten Bereichen bzw. Ortszonen und zu bestimmten Zeiten bzw. Zeitzonen. Hierdurch können z. B. Lieferanteneingänge, Verwaltungsräume, Entwicklungs- oder Produktionsbereiche vor unberechtigtem Zutritt geschützt werden. Nur die Personen erhalten Zutritt, die sich vorab zu erkennen gegeben haben, nämlich mit Ausweis, PIN-Code oder biometrischem Merkmal wie Fingerabdruck, Gesichts-, Iris- oder Venenerkennung. Zunehmend wird auch das Smartphone „als Türöffner“ mit einem digitalen Ausweis (z. B. in der Wallet) genutzt.



Zutrittssteuerung reicht vom Schutz einer einzelnen Tür bis zu sicherheitstechnischen und organisatorischen Gesamtmaßnahmen, etwa bei Großbetrieben.

Berechtigungen können für jeden einzelnen Ein- oder Ausgang unterschiedlich vergeben und gesteuert werden. So ist es z.B. möglich, dass eine bestimmte Person zu einem Raum ein unbeschränktes Zutrittsrecht hat, einen zweiten Raum nur zusammen mit einer weiteren Person betreten darf und eine dritte Tür nur innerhalb bestimmter Zeitzonen, z.B. werktags oder während der Geschäftszeiten, benutzen darf.

Somit bietet ein Zutrittssystem die Möglichkeit, Manipulationen durch Lieferanten und Personal oder Bedrohungen durch Fremde zu verhindern bzw. zu erschweren.

Zutrittssteuerung ist auch eine wichtige präventive Maßnahme, da potentielle Täter abgeschreckt werden. Sie kann zwar nicht verhindern, dass zutrittsberechtigte Personen (wie Mitarbeiter, Besucher und Lieferanten) kriminelle Handlungen begehen. Aber je nach Art der Zutrittsprotokollierung, die mitbestimmungspflichtig ist, können die Täter leichter identifiziert werden als ohne Zutrittssteuerung.

ZKT-14113-2025-12

Ein möglicher Verlust des Identifikationsmediums, wie Mitarbeiterausweis oder Transponder, ist weniger problematisch als beim herkömmlichen mechanischen Schließsystem, da die Ausweisnummer der verlorenen Zutrittskarte im System gesperrt wird, und nicht unbefugt zu nutzen ist.

Zutrittssysteme kommen in der Praxis in unterschiedlichster Form vor, die Bandbreite reicht vom einfachen mechatronischen Offline-Schließsystem, über vernetzte Online-Zutrittsleser bis zum Hochsicherheitssystem. Zunehmend werden auch Lösungen mit Smartphone angeboten. Damit können sich Mitarbeiter über eine App Over the Air (OTA) und digitale Wallets ausweisen, benötigen dafür ein NFC-fähiges Smartphone. NFC (Near Field Communication) erlaubt sichere Datenübertragungen über bis zu 5 cm und arbeitet mit einer Frequenz von 13,56 MHz, entsprechend dem ISO-Standard 14443A. Die Personenidentifikation sowie der verschlüsselt6e Datenaustausch zwischen Smartphone und Zutrittslesern kann wahlweise neben NFC auch per Bluetooth erfolgen.

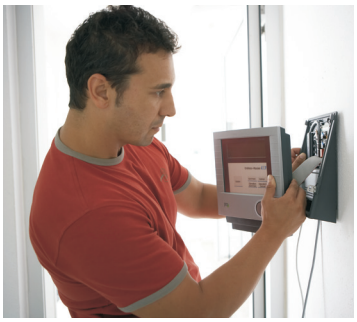
Die Zutrittssteuerung kann ein wertvoller Bestandteil der Sicherheits- und Gebäudeleittechnik sein. Neben der Anbindung von Einbruch- und Brandmeldeanlagen sowie der Videosicherheit werden meist auch Schnittstellen zur Fluchtwegsteuerung und zum Fluchtleitsystem, bis hin zu einem übergeordneten Gefahrenmanagementsystem angeboten.

Folgerichtig hat die Zutrittssteuerung auch Schnittstellen zu administrativen Systemen wie Zeit- und Betriebsdatenerfassung, Kantinen- und Tankdaten, Personaleinsatz- und Produktionsplanung, Ausweiserstellung und -verwaltung, Besucher-Management, Wächterkontrollsystem, Warensicherungssystem sowie zu Rechner- und Netzwerkzugängen.

2. Zutrittssteuerung kritischer Infrastrukturen (KRITIS)

Effektiver Schutz kritischer Infrastrukturen erfordert ausfallsichere und gezielte Zutrittssteuerung und umfassende Gefahrenmanagement-Lösungen. Bei der Umsetzung einer umfassenden Sicherheitslösung ist es wichtig, dass die einzelnen System-Komponenten nicht isoliert funktionieren, sondern in einem Schutznetz untereinander interagieren. Weil die Produkte oder Leistungen von KRITIS-Unternehmen von höchster Bedeutung für eine funktionierende Gesellschaft sind, muss das Risiko- und Sicherheitsmanagement entsprechend hohe Auflagen erfüllen. Um Risiken frühzeitig zu erkennen und Gefahren für kritische Infrastrukturen schnell und zuverlässig abwehren zu können, müssen Notfall-Szenarien und Folgeprozesse automatisiert zentral gesteuert werden. Bei dem Sicherheitskonzept für eine KRITIS-Institution sind viele Richtlinien und Einflussfaktoren zu beachten die im Praxisratgeber Zutrittssteuerung im Kapitel 7.6 beschrieben werden.

3. Planung und Realisierung der Zutrittssteuerung



Zutrittssteuerung ist eine technisch komplexe Aufgabenstellung mit großer Auswirkung auf Sicherheit, Organisation und Arbeitsabläufe eines Unternehmens. Damit sie für alle Beteiligten zufriedenstellend arbeiten kann, ist eine sorgfältige Planung und Errichtung durch qualifizierte Fachfirmen notwendig. In dieser Phase ist eine intensive Kommunikation zwischen Interessent bzw. Betreiber einerseits sowie dem Planer oder Errichter andererseits unverzichtbar. U.a. muss sich intensiv mit der Einordnung der technischen Systeme in die organisatorischen Abläufe des Unternehmens auseinander gesetzt werden. Interessenten an einer Zutrittssteuerungsanlage sollten sich deshalb zunächst einen Gesamtüberblick über den Nutzen und die Ziele verschaffen.

Gemäß Betriebsverfassungsgesetz und Datenschutz-Grundverordnung (DS-GVO) ist die betriebliche Zutrittssteuerung, insbesondere die Erfassung personenbezogener Daten, in Deutschland mitbestimmungspflichtig. In der Praxis muss daher die Arbeitnehmervertretung frühzeitig über eine geplante Zutrittssteuerung informiert werden, damit sie ihre Vorstellungen einbringen und mit dem Arbeitgeber eine Betriebsvereinbarung abschließen kann.

Bei der Planung und Realisierung einer Zutrittssteuerung sind Funktionen wie leichte Bedienbarkeit sowie akzeptable Reaktionszeiten des Systems zu berücksichtigen, um auch in Stoßzeiten einen schnellen Durchgang sicherzustellen. Weitere wichtige Punkte sind die Einbeziehung ggf. vorhandener Fluchtweg-Systeme, die Integration eines Videosicherheitssystems an sicherheitskritischen Zutrittspunkten, die logische Integration von Offline-Türterminals sowie die Einhaltung relevanter mechanischer Anforderungen für einen Betrieb mit möglichst langen Service-Intervallen.

Auch der Benutzerkomfort von Zutrittssystemen ist ein wichtiges Auswahlkriterium. Heute werden überwiegend RFID-Identkarten für berührungsloses Lesen genutzt. Hiermit kann - durch ein flexibles Speichermanagement auf der RFID-Identkarte - der Wunsch des Betreibers nach möglichst nur einer einzigen Identkarte für unterschiedliche Anwendungen im Betrieb, z.B. für Zutritt, Kantinenabrechnung, Zeiterfassung etc. leicht erfüllt werden. Durch die heutzutage oft eingesetzten biometrischen Erkennungsverfahren erübrigt sich oftmals die Verwaltung von PINs und Passwörtern.

Datenschutz-Grundverordnung

Wie für jedes IT-System gelten auch für die Zutrittssteuerung die Vorgaben der DS-GVO in Bezug auf Datenschutz und Datensparsamkeit (Verordnung (EU) 2016/679 vom 27. April 2016).

Normen/Richtlinien auf deutscher und europäischer Ebene

- **DIN EN 60839-11-1 (VDE 0830-8-11-1)** „Alarmanlagen - Teil 11-1: Elektronische Zutrittskontrollanlagen - Anforderungen an Anlagen und Geräte“ liegt als deutsche Fassung EN 60839-11-1:2013 mit zwei Berichtigungen vor.
- **DIN EN 60839-11-2 (VDE 0830-8-11-2)** „Alarmanlagen - Teil 11-2: Elektronische Zutrittskontrollanlagen - Anwendungsregeln“ liegt als deutsche Fassung EN 60839-11-2:2016 mit einer Berichtigung vor.
- **DIN EN 60839-11-31, -32, -33**: Diese geplante Normenreihe umfasst u.a. das Basis-Kommunikationsprotokoll sowie die Überwachung der Zutrittssteuerung, basierend auf Web-Services. Die Papiere liegen Stand 09/2018 nur teilweise vor und befinden sich noch beim IEC in Bearbeitung. Eine Veröffentlichung erfolgt, sobald alle 3 Teile fertig vorliegen.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- **Technische Richtlinie TR-03126-5** „Einsatzgebiet: Elektronischer Mitarbeiterausweis“
  Diese enthält u.a. Hinweise für die sichere Gestaltung von Zutrittskontrollsystemen, Zeiterfassung, usw. in Verbindung mit RFID und ist auf der BSI-Webseite unter „Publikationen“, „Technische Richtlinien“ verfügbar.
- **Technische Leitlinien zur Zutrittskontrolle** fordern für Anlagen mit Sicherheitsgrad 4 nach EN 60839-11-1 grundsätzlich die Verwendung einer Zwei-Faktor-Authentisierung.

Richtlinien VdS

Aufgrund des Ausgabedatums dieser Dokumente enthalten sie Referenzen auf nicht mehr gültige Normen der Serie DIN EN 50133.

- **VdS 2358** „Richtlinien für Zutrittskontrollanlagen, Teil 1: Anforderungen“ liegt als VdS 2358: 2009-10 (02) vor.
- **VdS 2359** „Prüfmethoden für Anlageteile von Zutrittskontrollanlagen“ liegt als VdS 2359: 2008-11 vor.
- **VdS 2367** „Richtlinien für Zutrittskontrollanlagen, Teil 3: Planung und Einbau“ liegt als VdS 2367: 2004-06 vor.

4. Auswahl des Ident-Systems

Zutrittssteuerung teilt die Benutzer in Berechtigte und Nichtberechtigte ein. Als Basis für ihre Entscheidung muss sie erkennen können, wer ihre Dienste gerade in Anspruch nehmen will. Hierfür ist sie darauf angewiesen, dass sich die Nutzer kooperativ verhalten und sich identifizieren (mittels PIN, Ausweis oder biometrischem Merkmal).

Die Identifizierung, durch die der berechtigte Nutzer Zutritt erlangen will, gilt als Willenserklärung. Versucht ein nichtberechtigter Mitarbeiter mit einer entwendeten oder gefundenen Karte Zutritt zu erhalten, zieht dies laut Betriebsvereinbarung in der Regel ernste arbeitsrechtliche Konsequenzen nach sich.

Der Ausweis ist der „Reisepass mit Visum" in einer auf diese Weise gesicherten Firma. Damit eine Identifizierung nicht versehentlich, sondern nur willentlich erfolgen kann, werden bei den meisten heute verwendeten Identverfahren mit berührungslosen Lesern kurze Reichweiten bis max. 10 cm empfohlen und verwendet. Mit einer (technisch durchaus möglichen) Leser-Reichweite (Mid- oder Long-Range), die über 10 cm hinaus geht, könnte eine Identkarte (z.B. aktiver Transponder mit Batterie) ungewollt automatisch ausgelesen werden, obwohl der Nutzer in diesem Moment keine Identifizierung wünscht.

Bei der Auswahl des Identsystems sollten durch die Organisations-, Sicherheits- oder Personalabteilung einer Firma auch mögliche zukünftige Entwicklungen bedacht werden, z.B. ob die gewählte Kartentechnologie auch zukünftigen Anforderungen genügt. Moderne Identkarten-Konzepte auf RFID-Basis teilen den Speicher auf der Identkarte in Applikationsbereiche ein. Bei fachmännischer Realisierung können ohne Probleme Zeiterfassungs- oder Kantinenabrechnungssysteme eingeführt werden, die auf der gleichen Ident-Technologie basieren. Unter der Bezeichnung „RFID-, Proximity- oder Berührungslos-Verfahren" werden unterschiedlichste Systeme angeboten, die sich stark voneinander unterscheiden und inkompatibel sind. Wird dieser Punkt nicht genügend beachtet, müssen die Mitarbeiter der Firma später mehrere unterschiedliche Karten benutzen. Empfehlenswert sind verschlüsselte RFID-Ausweise, wie MIFARE DESfire und LEGIC Advant die der ISO/ICE 14443 entsprechen. Siehe dazu das BHE-Papier: „Risiken beim Einsatz von Identmedien – Der BHE klärt auf".

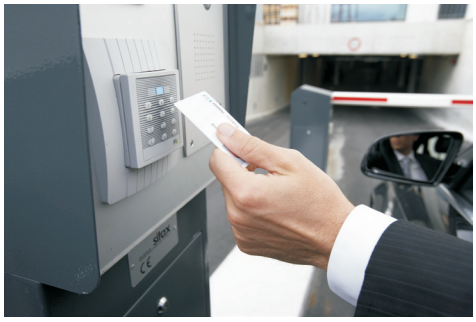
Ein biometrisches System bietet an einem besonders neuralgischen Punkt gegenüber anderen Identifikationssystemen, wie PIN und Ausweis zusätzliche Sicherheit: es stellt durch den 1:1-Vergleich mit sehr hoher Wahrscheinlichkeit fest, dass die per Biometrie verifizierte Person der rechtmäßige Besitzer der Karte ist. Unter Berücksichtigung der Datenschutz-Grundverordnung sollte das biometrische Merkmal (Template) statt in einer Datenbank auf einem RFID-Ausweis gespeichert werden. Mittels Verifikation (Ausweis plus biometrische Identifikation) kann darüber eine relativ sichere Personenidentifikation erfolgen.

5. Individuelle Risiko-Betrachtung

Eine erste Risikoanalyse kann vom Planer einer Zutrittssteuerungsanlage im Allgemeinen selbst durchgeführt werden, indem das Risikopotenzial, das der Betrieb bietet, realistisch-objektiv eingeschätzt und beurteilt wird. Kriterien können sein:

- Wie sieht die geografische Lage und das geografische Umfeld des Betriebes aus?
- Wie können sich potenzielle Angreifer den Gebäuden oder Gebäudeteilen nähern?
- Welches Potenzial bietet der Betrieb in Bezug auf Entwicklung und Forschung sowie die hergestellten/ verwendeten Produkte?
- Welche Schutzmaßnahmen existieren schon? Sind diese bereits bekannt bzw. sichtbar?
- Gibt es einen Sicherheitsdienst, Pförtner o.Ä.?
- Besteht Publikumsverkehr? Können Besucher sich im Gebäude frei bewegen?
- Gehört das Unternehmen zu einer regulierten Branche, wie KRITIS?
- Gibt besondere Sicherheitsauflagen aufgrund einer Zertifizierung, wie IFS Food, TISAX, Dora oder AEO?

6. Grundsätzliche Fragestellungen bei der Planung der Zutrittssteuerung



Zutrittssteuerung ist immer anlagenspezifisch zu planen. Dazu sind gute organisatorische und sicherheitstechnische Kenntnisse von Nöten.

Durch die Klärung grundsätzlicher Fragen bereits in der frühen Planungsphase kann das Zutrittssystem optimal dimensioniert werden.

Nachfolgend sind wesentliche Fragen aufgeführt, ohne Anspruch auf Vollständigkeit:

- Welcher Bereich (z.B. Innen- und/oder Eingangsbereich) soll abgesichert werden?
- Sollen einzelne Türen mit einem lokalen (Offline-)Zutrittssystem versehen werden? Um wieviele Türen handelt es sich? Sollen die dort erforderlichen Zutrittsrechte an online-Terminals auf den Ausweis geschrieben und laufend aktualisiert werden?
- Sollen die Türen bzw. Zugänge einem gemeinsamen Türmanagement, also einer übergeordneten Verwaltung (zentrale Mitarbeiter-Stammdaten) und einer zentralen Vergabe von Berechtigungen unterliegen oder sollen diese nur für eine oder mehrere einzelne Türen gelten, die dezentral mit Zutrittsdaten versorgt werden?

- Gibt es bereits Identkarten, ist das Kartenkonzept noch zeitgemäß oder besteht ein erhöhter Sicherheits- oder Speicherbedarf? Sind weitere kartengesteuerte Anwendungen geplant?
- Sollen neben dem Identkarten-Konzept auch zusätzlich geistige (PIN) oder biometrische Merkmale zur Erhöhung der Sicherheit (Zweifaktor-Authentifizierung) eingeführt werden?
- Gibt es schon eine Einbruchmeldeanlage, und wie erfolgt die Scharfschaltung?
- Wie hoch ist die Begehungsfrequenz? Im Durchschnitt und zu Spitzenzeiten?
- Ist eine Personenvereinzelung nötig? Sperre? Drehkreuz? Behindertengerecht?
- Ist eine automatische Schließvorrichtung geplant?
- Soll der Sicherheitsdienst die Sperre zentral und softwaregesteuert öffnen können?
- Ist eine Sprechanlage/Videokamera vorgesehen?

- Wird Material oder Gepäck befördert?
- Welche Maßnahmen werden zur Besucherregelung ergriffen?
- Ist eine Aufzugsteuerung mit Etagenwahl erforderlich?
- Gibt es Türkommunikationssäulen die in der ZK eingebunden werden sollten?
- Zufahrtskontrolle zum Gelände oder zur Tiefgarage berücksichtigen?
- Die Einbindung von Videosicherheitssystemen für neuralgische Punkte vorsehen?

7. Wichtige Hinweise zur Projektierung und typische Fehler

Die Erörterung und Klärung o.g. Fragen und aller weiteren Punkte, die aus der spezifischen Firmensituation resultieren, ermöglicht dem Planer, eine auf die gegebene Firmenstruktur angepasste Zutrittsanlage zu projektieren und einen langfristigen erfolgreichen Betrieb sicherzustellen.

Einige typische Ausführungsfehler bei der System- und Organisationsplanung:

- Identkarten-Konzept nicht umfassend geklärt
- Keine ausreichende Definition der max. Benutzerfrequenz
- Reaktionszeiten bei Belastung zu lang
- Türfallen- und -rahmenkontakte nicht berücksichtigt
- Verkabelung nicht rechtzeitig oder ausführlich geplant
- Material- und Gepäcktransport nicht bedacht
- Fluchtweg-Situation nicht geklärt / Nichtbeachten der Vorschriften für Fluchtwege
- Fehlende Einweisung und Motivation
- Verantwortung für den Betrieb der Anlage nicht definiert
- Nichtbeachten des Brandschutzes
- keine Einzelabsicherung am Elektro-Verteiler
- ungeschützte Leitungen im ungesicherten Bereich
- schlechte Bedienbarkeit der Zutrittsleser
- Nicht ausreichende Wartungsfähigkeit der Zutrittssteuerung
- Notstromversorgung für Stromausfall
- ungeeignete Mechatronik für Brandschutztüren

Organisatorisch und technisch gut geplante und richtig betriebene Zutrittsanlagen unterstützen das Managen von Gebäuden und Einrichtungen in erheblichem Maße. Dabei dienen sie nicht nur der „Security" der materiellen und immateriellen Güter, sondern auch der „Safety" der Betreiber und Benutzer der Anlage. Wegen der ständigen Nutzung der Zutrittsanlage haben die organisatorischen Belange und die Komfortansprüche der Benutzer neben den Sicherheits- und Sicherungsaspekten großen Einfluss auf die Planung und die Akzeptanz der Anlage. Mit ihrer Anbindung an andere Alarmsysteme und ihrer Verbindung zur Zeiterfassung ist das System zur Zutrittssteuerung ein wesentlicher Baustein der integrierten Gebäudeautomation.

Die BHE-Fachfirmen zeichnen sich durch ihre hohe Fachqualifikation aus und erfüllen alle Anforderungen, eine Zutrittssteuerungsanlage fachgerecht zu planen, zu installieren und instand zu halten. Interessenten finden sie unter www.bhe.de/fachfirmen-sicherheitstechnik

Der BHE-Fachausschuss Zutritt (siehe www.bhe.de/fachthemen/fachsparten/zutritt/infos-papiere) bearbeitet aktuelle Themen der Zutrittssteuerung und entwickelt zahlreiche praxisnahe Papiere. Die Papiere stehen zum freien Download bereit.

BHE-Praxisratgeber Zutrittssteuerung

Die 4. Ausgabe des Praxis-Ratgebers Zutrittssteuerung erläutert das komplexe Thema der Zutrittssteuerung in einfacher und verständlicher Weise. Er unterstützt Errichter, Planer und Anwender bei ihrer täglichen Arbeit und bietet einen echten Mehrwert. Neu- und Quereinsteigern der Zutrittssteuerung kann er als fundierte Einführung in das Thema dienen, Fortgeschrittenen als nützliches Nachschlagewerk. Bei der Überarbeitung wurde sehr viel Wert auf das Feedback der Leser gelegt und darauf aufbauend neben zahlreichen Erweiterungen, Aktualisierungen und Verbesserungen aufgenommen. Infos: www.bhe.de/publikationen/bhe-praxisratgeber/zutrittssteuerung.

BHE Bundesverband Sicherheitstechnik e.V.
Feldstraße 28
66904 Brücken
Telefon: 06386 9214-0
www.bhe.de, info@bhe.de