ZUTRITTSLÖSUNGEN

Sicher vor Manipulation?

Wie zuverlässig sind elektronische Zutrittssysteme? Unser Interview mit den BHE-Experten Axel Schmidt und Werner Störmer. Mit Tipps für Errichter, Integratoren, Betreiber und Endkunden

Zutritt elektronisch oder digital steuern - eine feine und komfortable Sache. Doch wie kann man sich gegen Manipulation schützen? Unser wissenschaftlicher Schriftleiter Heiner Jerofsky sprach mit dem Diplom-Wirtschaftsingenieur Axel Schmidt und mit dem ebenfalls diplomierten Ingenieur, Fachautor und Referent Werner Störmer. Die beiden sind jeweils Vorsitzender und stellvertretender Vorsitzender des Fachausschusses Zutritt im BHE Bundesverband Sicherheitstechnik. Die anerkannten Sicherheitsexperten des BHE nennen die Fakten – über neue Trends, Sicherheit, Hacking, Mechatronik, Biometrie und unterschiedlichste Sicherheitsniveaus bei der Zutrittstechnik.

GIT SICHERHEIT: Herr Schmidt, zunächst kurz zum BHE – was sind eigentlich die wichtigsten Aufgaben des Fachausschusses Zutritt?

Axel Schmidt: Das Ziel des FA-Zutritt im BHE ist die qualifizierte Bearbeitung des Themenbereiches Zutrittskontrolltechnik (ZKT) von verkabelten Online-Systemen über Funktechnologien, elektronischen Schließsystemen bis zu den Ausweis- und Identifikationssystemen. Der BHE ist somit kompetenter Gesprächspartner für alle Personen und Institutionen, die sich mit Fragen der Zutrittskontrolle (ZK), auch als Zutrittssteuerung bezeichnet, beschäftigen, (z.B. Mitgliedsunternehmen, Anwender, Behörden, Normungsgremien.

Die Aufgaben des FA Zutritt sind vielfältig:

- Erkennung und Beeinflussung aktueller Entwicklungen und Trends in der Zutrittssteuerung
- Erarbeitung von Anwendungspapieren, Broschüren und einem Praxis-Ratgeber
- Vorbereitung, Durchführung und Mitgestaltung von Seminaren und Kongressen
- Bearbeitung allgemeiner hersteller- und errichterspezifischer Problemstellungen im Bereich Zutritt
- Gedanken- und Erfahrungsaustausch inner- und außerhalb des BHE
- Erarbeitung von und Mitarbeit an Normen, Vorschriften und Richtlinien.

Diese Aktivitäten verbessern die Wettbewerbsfähigkeit der im BHE organisierten Fachfirmen für Zutrittskontrolle. Ihre Geschäftspartner vertrauen den hervorragenden Kompetenzen der BHE-Mitglieder, wodurch der wirtschaftliche Erfolg der Mitgliedsfirmen positiv beeinflusst wird.

Wo sehen Sie den wichtigsten Nutzen und die Einsatzmöglichkeiten von mechatronischen Schließsystemen?

Axel Schmidt: Die Abgrenzung mechatronischer Schließsysteme zu Offline- und Online-Systemen ist nicht mehr ganz zeitgemäß, der Übergang ist heutzutage meist fließend. Das mechatronische Schließsystem ist ein Teil – und für gewöhnlich ein ausgesprochen großer Teil – des Zutrittssystems. Mit den überwiegend batteriebetriebenen Komponenten (Beschläge, Zylinder, Vorhangschlösser, etc.) werden Gebäudeteile erreicht, die mit der klassischen online Zutrittskontrolle wirtschaftlich nicht abzubilden wären, vor allem sämtliche Türen, aber auch Schränke, Möbel, Wertfächer u.a.. Die Lebenszyklus-Kosten von offline ZK-Komponenten sind gegenüber einer mechanischen

Schließanlage geringer und die Sicherheit und Flexibilität nimmt überproportional zu.

Zutrittssysteme finden vielseitig Anwendung mit einer Vielfalt an Offline- und Online-Systemen. Können Sie den Unterschied, die Funktion und den Einsatz sowie die Vor- und Nachteile erklären?

Werner Störmer: Abhängig vom Sicherheitsgrad und den Gegebenheiten an einer Zutrittsstelle werden sowohl autonome als auch vernetzte Online-Zutrittssysteme angeboten. Autonome Terminals oder mechatronische Schließsysteme arbeiten eigenständig, ohne Verbindung zu einer übergeordneten ZK-Zentrale (ZKZ) und sind jeweils zuständig für eine Zutrittsstelle. Der Vorteil liegt in den geringen Installationskosten, jedoch fehlt meist die Möglichkeit, den Türstatus und die Alarmmeldungen (z.B. unberechtigter Zutrittsversuch) an eine zentrale Leitstelle zu senden. Nutzen, Einsatz- und Integrationsmöglichkeiten in vernetzte ZK-Systeme wurden bereits vorab von Axel Schmidt erläutert. Mehr Komfort und ein breiteres Einsatzspektrum bieten vernetzte Systeme mit einer übergeordneten Zutrittszentrale, an der abgesetzte Ausweis-/biometrische Leser oder ZK-Terminals sowie Vereinzelungseinrichtungen angeschlossen werden können. Zu beachten ist dabei die mögliche Anzahl und Art der Vernetzbarkeit (z.B. stern- oder busförmiger Anschluss, per Funk oder verkabelt) der anzuschließenden Zutrittsgeräte. Ansonsten sind folgende Eigenschaften erwähnenswert:

- schnelles Sperren von verlorenen Karten
- komfortable Eingabe, Weiterverarbeitung und Veränderung der gespeicherten Zutritts- und Berechtigungsdaten
- raumübergreifende Funktionen, wie die Wegüberwachung oder die automatische Steuerung von zentraler Stelle
- Integrationsfähigkeit anderer IT- oder kartengesteuerter Anwendungen.

Bei Aufteilung bestimmter Softwarefunktionen und Prüfungen in der ZKZ oder im ZK-Terminal, mit zusätzlicher Notstromversorgung, kann eine erhöhte Sicherheit erreicht werden. Bei Ausfall des ZK-Servers oder bei Leitungsunterbrechung(en) arbeitet die ZKZ oder das ZK-Terminal autark weiter, bis alle Systemkomponenten wieder funktionsbereit sind. Im Trend liegt die Verknüpfung von Zeit- und Zutrittssystemen ergänzt mit der Zufahrtskontrolle und Besucherverwaltung. Zur Kostenersparnis kann die Nutzung des gleichen Netzwerks, Ausweis- und Identifikationssystems, ggf. auch des gleichen Terminals sinnvoll sein. Mit nur einem Buchungsvorgang kann der Arbeitsbeginn des Mitarbeiters erfasst und die Zutrittsberechtigung erteilt werden. Ein weiterer Vorteil ist die Nutzung gleicher Stammdaten mit den Buchungs- und Zutrittsberechtigungen des Mitarbeiters. Vernetzte ZK-Systeme sind meist Teil eines integralen Sicherheitskonzepts mit Einbruchmeldesystemen, Videoüberwachung und zentraler Leittechnik. Hierzu gehört auch die Anbindung und Steuerung von Vereinzelungseinrichtungen, wie Drehkreuze, Durchgangsschleusen und Schranken.

Axel Schmidt

Werner Störmer

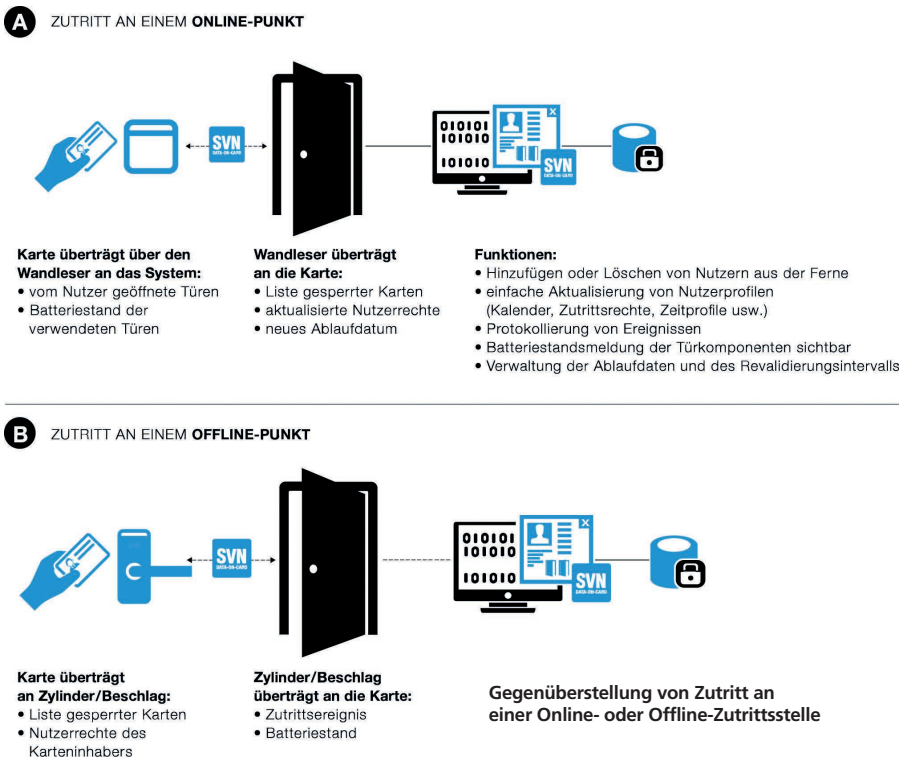
Zunehmend werden funkvernetzte, Cloud- und Smartphone-basierte bzw. mobile Zutrittssysteme angeboten. Wo liegen die Vor- und Nachteile gegenüber den klassischen, vernetzten Zutrittssystemen?

Axel Schmidt: Ein wesentlicher Nachteil der Offline ZK-Komponenten ist, dass sie eben offline sind und keine Verbindung zum Host-System besitzen. Um diesen Nachteil abzuschwächen, wurden schon im letzten Jahrzehnt die virtuellen Netzwerke entwickelt, in denen die Informationen über das Identifikationsmittel im Schneeballprinzip verteilt und gesammelt werden. Nachdem dann auch in der Funktechnologie batteriebetriebene Lösungen entwickelt wurden, kam der Ball ins Rollen. Das Smartphone ist ein nicht wegzudenkender Teil unseres Lebens geworden und mit BLE (BlueToothLowEnergy) ist ein Standard vorhanden, der flächendeckend zur Zutrittssteuerung genutzt werden kann. Auch die Entwicklung der Online-ZK geht von den Urmodellen über browserfähige-Systeme in Richtung Cloud. Die großen Softwareunternehmen (Microsoft, SAP, DATEV..) zeigen schon seit Jahren, dass Cloud-basierte Software die Zukunft ist. ZK ist Teil der Digitalisierung. Das Resultat wird sein: mehr Nutzer, mehr Daten, mehr Flexibilität und mehr Sicherheit.

Smartphones werden immer beliebter, wenn es um Zutrittslösungen geht. Wie sehen Sie die Entwicklung, auch im Hinblick auf die hiesigen Gegebenheiten, die Mentalität der Nutzer und die rechtlichen Aspekte?

Axel Schmidt: Als Chance und Risiko zugleich. Die Chance ist ein ständig verfügbares Medium mit Online-Funktion, das mit BLE, NFC, HCE usw. immer fast alle Technologien onboard hat. Als Risiko sehe ich vor allem den unzureichenden Schutz vor Manipulationen, Hackern, Datenklau usw., insbesondere bei unqualifizierten Entwicklungen und Produkten. Dem Nutzer muss es ermöglicht werden, eindeutig erkennen zu können, ob es sich um professionelle Sicherheitstechnik oder unzuverlässige SmartHome-Technik handelt.

Werner Störmer: Aus meiner Sicht sind zwar die Anwendungsmöglichkeiten von Smartphones in und zur Zutrittssteuerung vielversprechend, aber nicht für alle Firmen, Einsatzbereiche und Benutzerkreise geeignet. Beispielsweise ist in medizinischen Einrichtungen und spionagegefährdeten Abteilungen die Mitführung von Smartphones untersagt. Zu beachten sind auch die rechtlichen Aspekte, der Umgang mit personenbezogenen Daten und die Mitbestimmungspflicht. Man hat kaum Einfluss darauf, was ein Nutzer auf seinem Smartphone speichert und wie er damit umgeht. Als besonders kritisch sehe ich den BLE-Standard, der es Hackern ermöglicht, sich über die Funkverbindung einzuschleusen und ggf. die Kontrolle über das Gerät zu übernehmen. In einem Radius bis zu 10 m besteht außerdem die Gefahr, dass eine berechtigte Person mit ihrem Smartphone eine oder mehrere nahegelegene, gesicherte Türen mittels



BLE freigibt und Unberechtigte durchgehen können. Meiner Meinung nach werden sich Unternehmen aufgrund des Aufwands und der Kosten für die Umstellung kaum vom bewährten Ausweis trennen. Bestes Beispiel dafür ist der seit 1950 genutzte Magnetstreifenausweis im Zahlungsverkehr. Trotz neuer Technologien wie Chip, NFC und BLE beim Smartphone ist eine flächendeckende Ablösung noch lange nicht in Sicht.

Wie steht es um die Sicherheit vernetzter Systeme? Wie groß ist die Gefahr des Hackings?

> Im Trend liegt die Verknüpfung von Zeit- und Zutrittssystemen…

Werner Störmer: Um Schwachstellen des ZK-Systems abzusichern und gleichzeitig eine hohe Systemverfügbarkeit zu gewährleisten, sind mechanische, softwaretechnische, bauliche, elektronische und personelle Sicherungsmaßnahmen erforderlich. Systemabstürze oder Störungen, z.B. durch die Nichteinhaltung von Installationsanweisungen, kritische Umgebungsbedingungen, Stromausfälle oder Qualitätsmängel der eingesetzten Komponenten, sind wahrscheinlicher als die Gefahr, dass verschlüsselte Verbindungen gehackt werden. Zum Schutz der übertragenen Daten gegen Manipulation/Hacking kann eine Verschlüsselung auf verschiedenen Ebenen, beginnend mit der Identifikation (ID), der Datenübertragung bis zur Steuerungs- und Applikationsebene, erfolgen (s. Grafik oben):

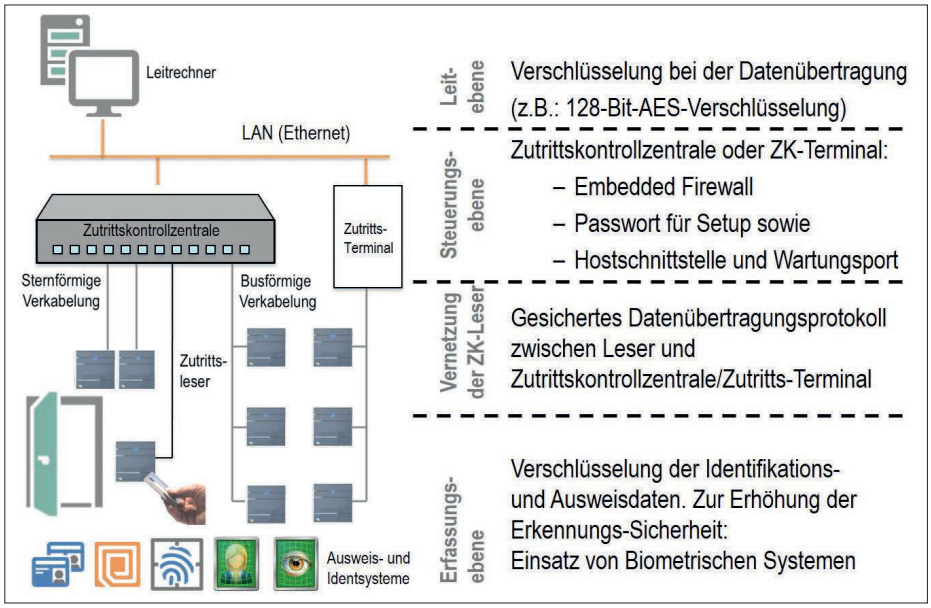
- Auf der Erfassungsebene: ID-Träger (Ausweis/biometrisches Merkmal) und der Datenaustausch mit dem ZK-Leser
- Bei der Übertragung auf den Datenleitungen: zwischen Erfassungsebene (ID-System/ZK-Leser/ZK-Terminal) und ZKZ sowie im LAN zwischen ZKZ und Applikationsserver
- Für eine definierte, geschlossene Benutzergruppe.

Ein vierstufiges hierarchisches Passwortkonzept kann dafür sorgen, dass die personenbezogenen, erfassten Daten vertraulich bleiben. Auf der untersten Ebene kann der Haustechniker mit seinem Passwort das Kommunikationsprotokoll konfigurieren oder die IP-Adressen beim Ethernetanschluss einstellen. Ein Betreuer kann zusätzlich Passwörter vergeben, Wartungsgruppen festlegen oder Parameter im ZK-Terminal ändern. Dem Systemverwalter auf der höchsten Sicherheitsstufe bleibt es beispielsweise vorbehalten, die Verschlüsselungen zu ändern und die Firewall im Terminal/Zutrittsmanager zu aktivieren. Eine sichere Zutrittskontrolle kann nur gewährleistet werden, wenn die aufgeführte Sicherheitskette keine Schwachstellen aufweist.

Personenidentifikation mittels Handvenenerkennung, integriert in einer Schleuse zur Zutrittssteuerung

Müssen wir uns Sorgen machen beim Smart Home?

Axel Schmidt und Werner Störmer: Smarte Produkte versprechen mehr Wohnkomfort und effizientere Energienutzung. Zahlreiche Anbieter wollen den Trend nutzen und werfen mit verlockenden Werbeaussagen unzählige kostengünstige Smart Home-Produkte auf den Markt. Doch Vorsicht: Bei solchen Produkten, die zum Selbsteinbau bestimmt sind und für wenige Euro im Internet bestellt oder im naheliegenden Baumarkt gekauft werden, ist vieles zu beachten. Nur selten erfüllen sie die sicherungstechnischen Qualitätskriterien, werden meist nicht „richtig“ installiert und verwendet. Zudem gaukeln sie den Bürgern totale Sicherheit vor, die mit den Systemen gar nicht erreicht werden kann. Für den Kunden sind die Unterschiede zwischen qualitativ hochwertiger Sicherheitstechnik und Billig-Produkten kaum zu erkennen. Verbraucher,



4-stufiges Datensicherheitskonzept in ZK-Projekten

> Für den Kunden sind die Unterschiede zwischen qualitativ hochwertiger Sicherheitstechnik und Billig-Produkten kaum zu erkennen.

deren Heim nicht nur „smart", sondern auch gegen Einbruch und Rauch geschützt sein soll, sollten eine qualifizierte Sicherheits-Fachfirma zu Rate ziehen. Sie kennt die entsprechenden Vorschriften, weiß welche Aspekte zu berücksichtigen sind und setzt professionelle Sicherheitssysteme ein. Damit die Systeme reibungslos arbeiten und zuverlässig schützen, sind einige Punkte zu beachten. Dazu bietet der BHE ein Info-Papier an, das unter www.bhe.de/sicheres-smart-home abgerufen werden kann.

Was bedeuten Unterschiede bei Sicherheitsniveau und Klassifizierung für den Einsatz von Zutrittslösungen? Was muss der Nutzer dazu wissen?

Axel Schmidt : In der aktuellen EN 60839-11-1 sind vier Risikograde vorgesehen. Die Einstufung nimmt der Betreiber anhand seiner Anforderungen an Sicherheit und Organisation sowie einer zuvor durchgeführten Risikoanalyse vor, ggf. gemeinsam mit dem Anbieter. Die Risikoanalyse ist nicht Gegenstand der Norm, aber hierzu wird eine Anleitung gegeben. Wesentlich ist außerdem der normative Anhang A, in dem Anforderungen der 4 Sicherheitsgrade aufgeführt sind, die nicht unbedingt in jeder installierten Anlage erfüllt sein müssen, wenn der Betreiber sie nicht benötigt. Die eingesetzten Systeme müssen aber die sicherheitsgradabhängigen Anforderungen erfüllen können. Diese Betrachtungsweise ergibt in der Praxis Zutrittskontrollanlagen, die mehrere bis alle Sicherheitsgrade aufweisen können. Die Normen behandeln nur das Zutrittssteuerungssystem mit seinen Schnittstellen zum Zutrittspunkt, zu den Benutzern, den Bedienern und zu anderen (Alarm)Systemen. Für die übrigen mechanischen Elemente gelten andere Normen.

In der Zeitschrift „SicherheitsPraxis" war Mitte 2017 ein kritischer Artikel, in dem behauptet wurde, dass es technisch möglich sei, jedes Schloss zu öffnen. Wie stehen Sie zu dieser These? Wie gut sind elektronische ZK-Systeme gegen Manipulation geschützt?

Axel Schmidt: Der Artikel mit den Aussagen von Herrn Di Filippo stellt die Mechanik- und Zutrittsbranche sehr negativ dar und ist für Anwender, Errichter oder Planer nicht hilfreich, sondern eher abschreckend. Nach diesen Aussagen müssten praktisch alle ZK-Systeme mit Online-Zugriff unsicher sein. Das ist Unsinn.

Werner Störmer: Es ist eine Binsenweisheit, dass man mit entsprechend hohem Aufwand nahezu jedes Schloss irgendwie öffnen kann. Absolute Sicherheit gibt es nun mal nicht. Wie viel kriminelle Energie man zur Öffnung oder Überwindung einer Zutrittsstelle benötigt, ist immer abhängig von dem realisierten Sicherheitsgrad. Im Hotel weiß ich, dass die Mitarbeiter in mein Zimmer kommen können (und im Notfall auch in den Zimmertresor), also verhalte ich mich auch entsprechend. Und in einer Firma ist es genau so. Eine Bäckereifiliale kann einfacher abgesichert werden als eine Bankfiliale. Wird ein Schloss oder eine Tür unberechtigt geöffnet, sollte die vernetzte Online-Türüberwachung einen Alarm auslösen. Außerdem werden in der Zutrittssteuerung nicht nur „Türschlösser" sondern z.B. auch Vereinzelungseinrichtungen mit Videoüberwachung eingesetzt. Die Statements von Assa Abloy, Primion Technology und PCS relativieren viele unstimmige Aussagen des Autors. Die u.a. im Artikel erwähnten klonbaren, nicht normgerechten Karten, die unverschlüsselten (Funk-) Verbindungen und die Smartphone-basierte ZK sind nur einem niedrigen Schutzgrad zuzuordnen. Eine sorgfältige Planung und gutes Fachwissen des Errichters gewährleisten, dass Sabotage, Manipulation und unberechtigte Zutritte weitgehend ausgeschlossen sind. Angefangen von der Personenidentifikation mittels gesicherter Ausweisverfahren und/oder biometrischer Merkmale, über einen verschlüsselten Datenaustausch auf allen Ebenen bis hin zur Notstromversorgung und passenden Perimeterschutz kann ein höchst möglicher Sicherheitsgrad erreicht werden.

Wie sicher sind die heute verfügbaren Ausweis- und Leseverfahren?

Werner Störmer: Hier hat sich die RFID-Technologie durchgesetzt. Sie bietet kontaktlose Identifikation (auch ohne Sichtkontakt), Kopierschutz, Verschlüsselung von Informationen und multifunktionalen Einsatz (Zeit, Zutritt, Login, Kantine, etc.), mit Schutz der Applikationen unter-/ gegeneinander. Fehlende Leseröffnungen, wie bei Einsteck- oder Durchzugsverfahren, erlauben auch den Einsatz in schmutziger Umgebung und reduzieren die Stör- und Manipulationsanfälligkeit. Relativ hohe Sicherheit bieten hier die verschlüsselten Technologien Mifare DESFire EV1/2 (AES-128) sowie Legic advant (DES/3DES).

Wie ist der Entwicklungstand und die Manipulationssicherheit bei den biometrischen Erkennungsverfahren?

Werner Störmer: Die biometrischen Verfahren sollen die Schwachstellen anderer ID-Methoden, wie „vergessener, verlorener oder beschädigter Ausweis", eliminieren. Als statische Verfahren in der Zutrittskontrolle werden heute Fingerabdruck, Handgeometrie, Venenerkennung, Iris und Gesicht eingesetzt. Bei der erstmaligen Benutzung, dem sogenannten Enrollment, werden die Kennwerte jedes Teilnehmers als Referenzdaten (template) gespeichert und bei der für die ZK erforderlichen Identifikation mit den aktuell aufgenommenen Messwerten verglichen. Bei Übereinstimmung und Zutrittsberechtigung

Grad	1	2	3	4
Risikograd	niedrig	niedrig bis mittel	mittel bis hoch	hoch
Anwendung	organisatorische Gründe; Schutz von Sachgegenständen mit geringem Wert	organisatorische Gründe, Schutz von Sachgegenständen mit geringem bis mittlerem Wert	weniger organisatorische Gründe, Schutz von kommerziellen Gegenständen mit mittlerem bis hohem Wert	hauptsächlich Schutz hochwertiger kommerzieller oder infrastruktureller Werte
Fertigkeiten/ Wissen der Angreifer	geringe Fertigkeit, geringes Wissen über ZKA, kein Wissen über Erkennungsmittel und IT-Technologien geringe finanzielle Mittel für einen Angriff	mittlere Fertigkeit und mittleres Wissen über ZKA, geringes Wissen über Erkennungsmittel und IT-Technologien geringe bis mittlere finanzielle Mittel für einen Angriff	hohe Fertigkeit und hohes Wissen über ZKA, mittleres Wissen über Erkennungsmittel und IT-Technologien mittlere finanzielle Mittel für einen Angriff	sehr hohe Fertigkeit und sehr hohes Wissen über ZKA, hohes Wissen über Erkennungsmittel und IT-Technologien hohe finanzielle Mittel für einen Angriff
Übliche Beispiele	Hotel	Wirtschaftsgebäude, kleine Firmen	Industrie, Verwaltung, Banken	Hochsicherheitsbereiche (militärische Einrichtungen, Regierungen, Forschungseinrichtungen, kritische Produktionsbereiche)

Risikograde lt. EN 60839-11-1

wird der Zugang freigegeben. Der gespeicherte Datensatz enthält keine „Rohdaten", wie Passbild oder Fingerabdruck, sondern nur die daraus extrahierten Merkmale, z.B. eine mathematische Beschreibung der Endungen und Verzweigungen der Fingerabdrucklinien beim Fingerprint oder des Iris-Musters bei der Iris-Erkennung. Eine der sichersten biometrischen Technologien ist die Handvenenerkennung. Im Gegensatz zum Fingerprint lässt sich das Venenmuster einer Handfläche nicht fälschen. Wird eine RFID-Karte der neuesten Generation zum Öffnen einer Vereinzelungsanlage mit der Handvenenerkennung in der Zutrittsschleuse kombiniert, lassen sich Zugänge so absichern, dass ein unbefugter Zutritt nahezu ausgeschlossen ist. Datenschutzprobleme entfallen weitgehend, wenn auf eine zentrale Speicherung des template verzichtet wird und die Anwender den Ausweis als Speichermedium der biometrischen Merkmale selbst verwalten. Denn die zentrale Speicherung birgt ein Missbrauchs- und Schadenspotential, z.B. durch Hacking. Da meist Ausweise schon für andere kartengesteuerte Anwendungen genutzt werden, kann bei sehr hohen Sicherheitsanforderungen die Ausweis-Eingabe mit der biometrischen Personenidentifizierung kombiniert werden. Aus Datenschutzgründen kann das template auf der RFID-Karte gespeichert werden.

> Eine der sichersten biometrischen Technologien ist die Handvenenerkennung.

Was tut der BHE, um Facherrichtern und Anwendern die Systeme und deren richtige Planung, Projektierung, Einsatz und Wartung zu vermitteln - um so vielleicht auch mehr Sicherheit im Umgang mit der Sicherheitstechnik selbst zu schaffen?

Axel Schmidt und Werner Störmer: Viel! Unter anderem bietet der BHE ein breites Angebot an Fachlektüre, Infomaterial, Seminaren und Kongressen.Besonders empfehlenswert ist der Praxis-Ratgeber Zutrittssteuerung. Gerne kann der BHE auch telefonisch oder per E-Mail kontaktiert werden. Kompetente Experten für Zutrittssteuerung finden Anwender immer beim BHE. Die BHE-Mitglieder sind für ihre hohe Fachkompetenz sowie gut geschultes und qualifiziertes Personal bekannt und zeichnen sich durch Fachkenntnis und Flexibilität aus. Verschiedene Filterfunktionen unter www.bhe.de/Fachfirmensuche erleichtern die Suche nach Fachfirmen. Hilfestellung bietet übrigens auch das Qualitätssiegel „BHE-zertifizierter Fachbetrieb". Entsprechend zertifizierte Unternehmen sind unter www.bhe.de/Fachfirma-zutritt zu finden.

Soviel zur heute verfügbaren Zutrittssteuerungstechnik und ihre Zuverlässigkeit – wir danken für das Interview.

BHE-Fachausschuss Zutritt

Die Fachausschüsse des BHE bearbeiten im Interesse der Mitgliedsunternehmen aktuelle Fragen und Aufgabenstellungen der Branche. Der Fachausschuss Zutritt befasst sich mit allen Fragen der Zutrittstechnik. Die Ergebnisse haben zweifellos positive Auswirkungen auf das gesamte Geschehen im in- und ausländischen Sicherheitsmarkt.

Links und weiterführende Informationen

- Fachwissen und sicherheitstechnische Informationen: www.bhe.de/BHE-Wissen
- Seminare: www.bhe.de/seminare
- Kongresse: www.bhe.de/kongresse.
- Praxis-Ratgeber Zutrittssteuerung (s. www.bhe.de/Praxis-Ratgeber-Zutritt)

Kontakt

BHE Bundesverband Sicherheitstechnik e.V.
Anke Sepp
Tel.: 06386 9214-11
E-Mail: a.sepp@bhe.de
www.bhe.de