

# Sicherheit durch Zutrittssteuerung

Über mechanische und elektronische Zugangssteuerungssysteme wurde bei einem Simedia-Forum umfassend informiert.

Von Zutrittskontrolle zu sprechen, ist eigentlich falsch. Man sollte vielmehr von Zutrittsregelung sprechen,“ sagte DI Jürgen Junghanns, *Interflex Daten-systeme GmbH*, zu Beginn des dreitägigen Forums „Modernes Zutritts- und Berechtigungsmanagement“ der *Simedia GmbH*, das vom 13. bis 15. November 2007 in Stuttgart stattgefunden hat. „Das englische Wort Access Control wurde falsch übersetzt; to control bedeutet eigentlich lenken, leiten, steuern“.

Dennoch hat sich der Begriff Zutrittskontrolle durchgesetzt. Sie ist ein Organisationsmittel, das Nichtberechtigte vom Zutritt ausschließen und Berechtigte so wenig wie möglich in ihrer Bewegungsfreiheit behindern soll.

Zutrittskontrolle beginne – abgesehen von der jeweiligen Ansteuerung – bereits bei den mechanischen Barrieren, wie etwa Zufahrten, Türen und Toren, erläuterte Diplomkaufmann Harald Seiffert von der „von zur Mühlen’schen GmbH“. Im Idealfall sollte derselbe Widerstandswert erreicht wer-



**Harald Seiffert:** „Zutrittskontrolle beginnt bei den mechanischen Barrieren wie Türen und Toren.“

den, wie die umgebende Wandkonstruktion. Die Überwindung dieser Hindernisse müsse nur mit definiertem Aufwand möglich sein, müsse auffallen, geplante Reaktionen auslösen und auch beweisbar sein.

„Scheinsicherheit ist eine der schlimmsten Formen der Unsicherheit“, betonte Seiffert im Hinblick darauf, wie leicht selbst „HiTech trivial“ unterlaufen werden kann. Beispielsweise findet man die Gitter von Toren so verschraubt, dass die Schrauben von der Angriffsseite her gelöst werden können, der Türdrücker von außen her durch Durchgreifen oder mit Hilfsmitteln



**Jürgen Junghanns:** „Man sollte vielmehr von Zutrittsregelung sprechen als von Zutrittskontrolle.“

betätigt oder das Zugseil zur Toröffnung bei Tiefgaragen von außen erreicht werden kann. Die Funktion eines elektrischen Türöffners, der in der Regel lediglich auf die Falle des Schlosses wirkt und diese bei Betätigung freigibt, kann durch den Entriegelungshebel („Tagesfalle“) außer Funktion gesetzt werden. Wenn, wie bei Fluchttüren, Türöffner nach dem Ruhestromprinzip arbeiten, reicht eine Unterbrechung der Stromzufuhr zum Öffnen aus – leicht möglich, wenn die Leitung nicht unter Putz, sondern auf Putz verlegt ist. Bei einer geöffneten Tür sollte überwacht werden, ob

sie auch wieder schließt oder geschlossen wird.

Stumpfe Türblätter, die auf der Angriffsseite keinen Falz aufweisen, ermöglichen es, die Falle zurückzuzwängen, was den Türöffner hilflos macht, gleichgültig, mit welchen noch so aufwendigen Verfahren er angesteuert wird.

Auch das Umfeld ist in die Planung von Zutrittskontrollsystemen einzubeziehen. Wo haben sich „By-pässe“ entwickelt, indem etwa über offen gehaltene (verkeilte) Fluchttüren, bei der Warenannahme, über Monteurzugänge, Raucher-ecken im Außenbereich, unkontrollierter Zutritt möglich ist? Wo befinden sich verdeckte Bereiche wie etwa begehbbare Schächte oder im Technikbereich? Oder es werden Maßnahmen der Zutrittskontrolle kurzzeitig außer Kraft gesetzt – wie beispielsweise zur Kantenzeit.

**Systeme.** Das geläufigste Zutrittskontrollsystem ist der Schlüssel, der dem Inhaber, ob berechtigt oder nicht, den Zutritt öffnet. Das Konstruktionsprinzip des

## SIMEDIA GMBH

**Die Simedia GmbH,** Bonn, ein Unternehmen der „von zur Mühlen-Gruppe“, vermittelt die Erfahrungen der Tochtergesellschaften bei der Planung von Rechenzentren und der Sicherheitsberatung in Form von Kongressen, Konferenzen, Foren, Seminaren und Workshops zu nahezu allen Bereichen unternehmerischer Sicherheit. Das Pro-

gramm des Jahres 2008 ist geprägt durch die Lehrgänge „Krisenmanagement für Führungskräfte“ (Grund- und Aufbaulehrgang) sowie „Notfallmanagement für Führungskräfte“. Dazu kommen die Lehrgänge Objektsicherheit I bis III, mit denen dazu übergegangen wurde, breites Grundlagenwissen auf dem Gebiet der Sicherheitstechnik und -pla-

nung praxisnah zu vermitteln, unter Einbeziehung kaufmännischer und wirtschaftlicher Gesichtspunkte. Bei einer abschließenden Prüfung besteht die Möglichkeit, das Zertifikat des Bundesverbandes unabhängiger deutscher Sicherheitsberater und -ingenieure als „Security Engineer, BdSI“ zu erlangen. Mit der am 1. April 2008 in Frankfurt be-

ginnenden Veranstaltungsreihe „Sicherheits-Wissen kompakt“ werden in eintägigen Seminaren sowohl Erfahrungswissen aus konkreten Projektberichten als auch Kenntnisse zum Vorgehen in Projekten (z. B. Analysen, Konzeption, Umsetzungsplanung) im Rahmen von Gruppenarbeiten erworben.

[www.simedia.de](http://www.simedia.de)

Schließzylinders ermöglicht es, Schließhierarchien mit entsprechenden Verästelungen einzurichten. Der Verlust oder die Kompromittierung eines übergeordneten Schlüssels zieht nach sich, dass die untergeordneten Schlösser ausgetauscht werden müssen – was bei Verlust eines Generalschlüssels hohen finanziellen Aufwand bedeuten kann.

Die Informationstechnologie schafft Abhilfe und bietet neue Anwendungsmöglichkeiten. Über Datenträger und entsprechende Lesegeräte sowie Auswertungseinheiten können nicht nur Zugänge geöffnet werden, es kann auch festgelegt werden, wer Zutritt hat (Mitarbeiter, Fremdpersonal, Besucher); wann (werktags, feiertags, tagsüber, nachts, einmalig, für Veranstaltungen); wo (Betriebsgebäude, Parkplatz, Produktion, Entwicklung, EDV). Der Trend geht dahin, Mitarbeiter nach „Vertrauensklassen“ einzuteilen, damit bei Unternehmen mit verschiedenen Standorten nicht jeweils neue Zutrittsberechtigungen erteilt werden müssen. Allerdings sollte das „Need-to-Know-Prinzip“ herrschen und die Zutrittsberechtigung nicht von der persönlichen Stellung in der Unternehmenshierarchie abhängig gemacht werden.

Die Systeme können zur Zeiterfassung genutzt werden, zum Zugriff auf Daten und Programme, zur Inbetriebnahme von Geräten (Drucker, Kopierer; Fahrstuhl, Stapler), zur Parkplatzbewirtschaftung oder Abrechnung in der Kantine oder an Automaten. Zutritte können protokolliert werden; bei Verlust eines Datenträgers kann dieser ohne großen Aufwand gesperrt werden.

Eine Verbindung mit einer Videoüberwachungsanlage (CCTV), der Ein-



**Über Datenträger und entsprechende Lesegeräte sowie Auswertungseinheiten können nicht nur Zugänge geöffnet werden, es kann auch festgelegt werden, wer Zutritt hat.**

bruchsmeldeanlage und in weiterer Folge mit der Sicherheitsleitstelle ist sinnvoll, denn nur so kann erkannt werden, warum ein Zugang geöffnet ist (Sabotage, Einbruch), weshalb rasch aufeinanderfolgend Fehleingaben erfolgen oder welche Situation vorliegt, wenn über die Tastatur ein Bedrohungscode eingegeben wird. Allerdings müssen dann auch Pläne vorliegen, wie in diesen Fällen zu reagieren ist.

Als Datenträger sind Karten mit Magnetcode überholt und werden durch Chipkarten abgelöst, die eine Speicherung größerer Datenmengen als bei Magnetkarten zulassen, ebenso eine Aufteilung des Speicherplatzes in voneinander getrennte Bereiche für verschiedene Anwendungen. Außerdem können die gespeicherten Daten vor unberechtigtem Zugriff (Lesen) geschützt werden, unberechtigtem Ändern (Verfälschen) und vor Duplizieren oder Kopieren. Chipkarten

auf Kontaktbasis sind verschleißanfällig. „Der Renner“ sind berührungslos über RFID arbeitende Chipkarten. Sie sind unempfindlich gegenüber äußeren Einflüssen; die Ausweisleser können vandalismussicher und wetterfest gestaltet werden. Die Daten können im üblichen Frequenzband von 13,56 MHz auf eine Entfernung bis etwa 50 Zentimetern, in einem Gate bis einem Meter ausgelesen werden; in Verbindung mit passiver UHF auch auf mehrere Meter und somit auch aus einem langsam fahrenden Fahrzeug heraus.

Der Besitz einer solchen Karte allein bedeutet allerdings nicht, dass der Inhaber zum Zutritt berechtigt ist. Die Karte könnte gestohlen, an Unberechtigte weitergegeben oder gefälscht worden sein. Um die tatsächlich gegebene Berechtigung nachprüfen zu können, könnte zusätzlich Wissen abgefragt werden, etwa die Kenntnis der PIN oder eines Passworts. Auch dieses

Wissen kann ausgehorcht, ausgespäht oder weitergegeben worden sein oder ist schlichtweg durch Vergessen verloren gegangen.

**Biometrie.** Sich der Person des Berechtigten mit größtmöglicher Sicherheit zu vergewissern, gelingt mit dessen individuellen körperlichen Merkmalen, die andererseits der Art nach wieder so allgemein sein müssen, dass sie im Prinzip auf alle Menschen zutreffen (Universalität). Zudem dürfen sich diese Merkmale im Zeitablauf entweder nicht oder nur sehr langsam ändern. Die Person selbst wird dann zum Träger der Erkennungsinformation; aus Personenbezogenheit wie beim Ausweis wird Personengebundenheit.

Im Speziellen haben sich an geeigneten biometrischen Merkmalen physiologische (statische) wie Fingerabdruck, Handflächengeometrie, Gesichtserkennung zwei- und dreidimensional sowie Iriserkennung am



**Zutrittskontrolle durch Magnetkarte.**

Markt durchgesetzt. Erkennung des Augenhintergrunds (Retina), Venenstruktur, Gesichtstemperatur, Geruch oder die Geometrie der Ohrklappen sowie verhaltensorientierte (dynamische) Erkennungsmethoden (Stimme, Unterschrift, Lippenbewegung, Gang, Rhythmus der Tastatureingabe) sind in den Hintergrund getreten.

Die Erkennung über Fingerabdruck ist laut Jürgen Junghanns erprobt, hat einen Marktanteil von knapp 40 Prozent, ist schnell und preisgünstig, versagt allerdings beispielsweise bei verschmutzten Händen (Werkstättenbereich) und ergibt in etwa ein bis zwei Prozent der Fälle keine Auswertung (Verletzungen, Abrieb u. a.). Hier eignet sich die Vermessung der Handflächengeometrie besser; sie ist ebenfalls schnell und preisgünstig, sozial akzeptiert, mit sehr hoher Markterfahrung und einem Marktanteil von 27 Prozent, doch die Lesegeräte sind größer und sollen für Links- und Rechtshänder geeignet sein. Die zweidimensionale Gesichtserfassung hat einen Marktanteil von 13 Prozent, erfordert eine ziemlich konstante Beleuchtung und erlaubt nur geringe Abweichungen der Positionierung des Gesichtes beim Hinse-

hen. Diese Nachteile vermeidet die dreidimensionale Gesichtserfassung, doch liegt hier nur sehr wenig Markterfahrung vor und auch dieses System ist relativ teuer. Die Iriserkennung (Marktanteil einschließlich Retina-Erkennung etwa 15 Prozent) ist sehr selektionsfähig, allerdings ebenfalls eher teuer, bei bereits guter Markterfahrung.

Biometrische Verfahren werden nicht nur für Hochsicherheitsanlagen eingesetzt, sondern dienen auch nur dazu, um Mängel in der Ausweisorganisation (vergessene Ausweise) auszugleichen. Biometrische Verfahren sind fehleranfällig, weil das gespeicherte Abbild nicht zu 100 Prozent wiederholt werden kann. Die False-Rejection-Rate (FRR) gibt an, zu welchen Prozentsätzen Berechtigte abgewiesen werden; die False-Acceptance-Rate (FAR), zu welchem Prozentanteil Unberechtigte durchgelassen werden. Die FAR liegt bei herkömmlichen Verfahren bei 0,1 Prozent, bei 3-D-Gesichtserkennung bei 0,02 Prozent und bei Iriserkennung bei 0,00003 Prozent; die FRR bei allen Verfahren zwischen 0,2 und 0,7 Prozent. Durch entsprechende Einstellungen im Programm können diese Werte gegeneinander verschoben wer-



**Die Erkennung über Fingerabdruck ist erprobt, schnell und preisgünstig, versagt allerdings beispielsweise bei verschmutzten Händen.**

den, wobei zu überlegen ist, welcher Fehler schlimmer ist. Die Equal-Error-Rate ergibt sich am Schnittpunkt der beiden Kurven und stellt die optimale Einstellung der Anlage dar.

Biometrische Verfahren sind rechenintensiv und eignen sich hauptsächlich für Verfahren zur Zutrittskontrolle, bei denen sich jemand über Ausweis oder PIN schon zu erkennen gegeben hat und nun überprüft werden soll, ob er tatsächlich derjenige ist, als der er sich ausgibt (Verifikation). Zur Identifikation, also aus einer mehr oder weniger großen Menge jemandem eine abgespeicherte Identität zuzuordnen, eignen sie sich nur bedingt, weil sich, näherungsweise dargestellt, die bei jeder Person gegebene Rate der Falschakzeptanz mit der Anzahl der Personen multipliziert. Allenfalls können zu Zwecken der Zutrittskontrolle die Verfahren kombiniert werden, dass also eine Vorprüfung durch Identifikation vorgenommen wird und nachfolgend nur mehr eine Verifikation vor-

genommen werden muss. Zu unterscheiden sind auch kooperative Verfahren, die eine bewusste Handlung voraussetzen, oder nichtkooperative, wie sie beispielsweise auf öffentlichen Plätzen eingesetzt werden und ohne Wissen oder sogar gegen den Willen des Betroffenen zu einer Identifizierung oder einem Identifizierungsvorschlag führen.

Letztlich wurden eingehend auch die sicherheitstechnischen Schwächen von RFID-basierten und von biometrischen Systemen erörtert. Sie bieten Angriffsmöglichkeiten und können überlistet oder ausgeschaltet werden. Es wurden auch Abwehrmaßnahmen entwickelt wie etwa die Lebenderkennung oder kryptografische Verfahren für die Funkstrecke bei RFID.

Verglichen mit den Schwächen von Ausweissystemen in der analogen Welt (Ausweise können leicht ge- oder verfälscht werden), wird aber in der digitalen Welt ein beträchtlicher Sicherheitsgewinn geboten.

*Kurt Hickisch*