Ohne Schlüssel

Beim Simedia-Forum „Modernes Zutritts- und Berechtigungsmanagement“ wurden neue Lösungen zur Zutrittskontrolle präsentiert.

Kann man sich ein Geldinstitut vorstellen, in dem es weder Schloss noch Schlüssel gibt, keine Ausweiskarten und in dem dennoch ein Höchstmaß an Sicherheit für Kunden und Mitarbeiter gegeben ist? Zudem soll ein solches System auch zur Zeiterfassung, für Verkaufsautomaten und für die logische Zugriffskontrolle geeignet sein.

Biometrie macht derartiges möglich, und verwirklicht wurde ein solches System bei der Schweizer Privatbank *Pictet & Cie, Banquiers,* die diese Forderungen beim Neubau des Verwaltungsgebäudes in Genf erfüllt sehen wollte. Der Sicherheitsberater Dipl.-Ing. Jürgen Junghanns berichtete über die Umsetzung dieses Konzepts beim *Simedia*-Forum „Modernes Zutritts- und Berechtigungsmanagement“, das am 25. und 26. November 2008 in Berlin stattfand, mit einem Workshop am 27. November.

Grundsätzlich können zur Zutrittsregelung „Besitz“ (Schlüssel, Ausweiskarte), Wissen (PIN, Kennwort) sowie biometrische Merkmale herangezogen werden. Besitz an Dingen kann verloren gehen, auch ein Unberechtigter kann sie verwenden. Schlüssel oder Karten können kopiert werden. Wissen kann vergessen, weitergegeben oder ausgespäht werden. Mit dem Menschen untrennbar verbunden sind biometrische Merkmale, die sich ihrerseits wieder in solche unterteilen lassen, die physiologisch (Gesicht, Handgeometrie, Fingerabdruck, Irismuster, Netzhaut, Venenmuster) oder verhaltensorientiert (Stimme, Lippenbewegung, Unterschrift, Tastatureingabe, Gang) sind.

Zur Zutrittsregelung können Ausweise sowie biometrische Merkmale herangezogen werden.

Wichtig ist bei biometrischen Merkmalen, dass jeder Mensch dieses Merkmal besitzt (Universalität); dass das Merkmal zwar für ein und dieselbe Person eindeutig, aber von Person zu Person verschieden ist; dass die Merkmale entweder konstant sind oder sich im Zeitablauf nur langsam ändern, und dass sie messbar sind.

Eine hohe Wahrscheinlichkeit der Einmaligkeit ist gegeben bei Fingerabdruck, Irismuster und Augenhintergrund (Retina). Selbst eineige Zwillinge weisen unterschiedliche Irismuster und unterschiedliche Fingerabdrücke auf.

Biometrische Erkennungsverfahren haben den Nachteil, dass das zu prüfende Muster nie genau mit dem hinterlegten Referenzbild übereinstimmt. Im Gegenteil, es wäre ein Alarmkriterium, würde nach Form und Lage genau derselbe Fingerabdruck präsentiert werden, denn dann wurde ein zuvor eingelesener Fingerabdruck offenbar zu Täuschungszwecken aktiviert und neuerlich verwendet.

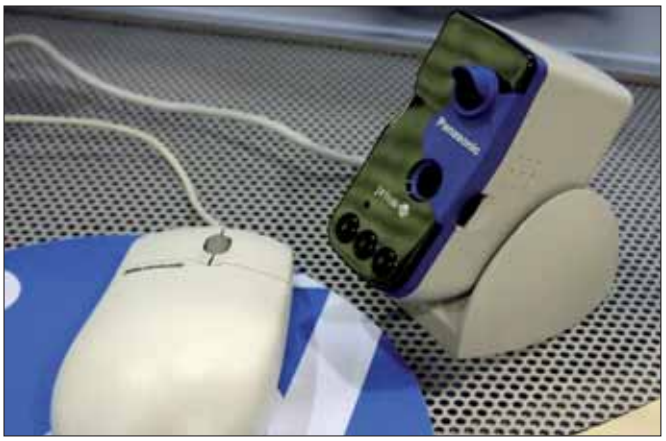
Fehlerrate. Bei biometrischen Erkennungssystemen wird es immer eine Fehlerrate geben, entweder wird ein Berechtigter vom System fälschlicherweise zurückgewiesen („False Rejection Rate“, FRR) oder ein Unberechtigter erhält Zutritt („False Acceptance Rate“, FAR). Die Frage ist, was ist schlimmer, Berechtigte (allenfalls auch Vorstandsdirektoren) irrtümlich zurückzuweisen oder Unberechtigte zuzulassen. Die jeweiligen Toleranzen sind einstellbar und einander gegenläufig; das Gleichgewicht ist dann erreicht, wenn die Rate der Zurückweisungen Berechtigter gleich der der Zulassung Unberechtigter ist.

Biometrische Verfahren erfordern eine längere Rechenzeit, sodass sie zumeist zur Verifikation eingesetzt werden, also zur Überprüfung, ob jemand tatsächlich der ist, als der er sich zuvor durch einen Ausweis oder durch Eingabe einer PIN ausgegeben hat (Vergleich 1:1; One-to-one-Matching). Bei einer Identifikation, dass also in einer Datenbank gesucht werden muss, ob die präsentierten biometrischen Merkmale zu den abgespeicherten Referenzdaten passen (Vergleich 1:n; One-to-many-Matching), dauert die Suche länger.

Die erwähnte Schweizer Bank hat dennoch und weltweit einzigartig auf ein Identifikationssystem gesetzt, entsprechend der Vorgabe, dass keine Art von Ausweisen erforderlich sein soll, nicht einmal berührungslos funktionierende. Im Eingangsbereich der Bank wird 3-D-Gesichtserkennung mit „Licht“ im nahen Infrarotbereich eingesetzt; Speedgates ermöglichen den reibungslosen Einlass auch zu Stoßzeiten. Die Identifikation ist in weniger als einer Sekunde abgeschlossen. Für innere Hochsicherheitsbereiche, wie etwa Tresorräume und Rechenzentren kommt Iriserkennung zum Einsatz.

2004 wurde unter dem Generalunternehmer *Interflex AG Schweiz* mit den ersten Planungen begonnen, 2005 wurde mit etwa 400 Mitarbeitern unter Echtzeitbedingungen das System durch mehrere Monate getestet, auch die Akzeptanz. Ab 2006 wurde schrittweise in den Echtbetrieb übergegangen, der im Februar 2007 erreicht wurde. Seither sind alle rund 2.600 Mitarbeiter in das System eingebunden, das auch eine Zeiterfassung ermöglicht. Für die Zufahrt zu den Parkplätzen und zur Tiefgarage wurde eine Kennzeichenerkennung installiert, die immerhin drei Arten von Schweizer Kennzeichen und französische zu verarbeiten in

FOTO: METALLBAU-KLAUENBERG



Irisscanner: Hohe Wahrscheinlichkeit der Einmaligkeit ist gegeben bei Irismuster und Augenhintergrund (Retina).

Wireless-Key-Zutrittssystem: Bluetooth-fähiges Handy als Schlüssel.

der Lage sein muss. Die Gesamtkosten des Systems lagen etwa 15 bis 20 Prozent höher als bei einer „normalen" Anlage, doch dürften die Kosten des laufenden Betriebes geringer sein.

Handvenenerkennung. Der Einsatz biometrischer Erkennungsverfahren ist auch davon abhängig, unter welchen Bedingungen sie zum Einsatz kommen sollen. Kommt ein Personenkreis in Betracht, bei dem etwa mit verschmutzten Händen zu rechnen ist (Werkstätten, Mechaniker), sind Fingerprints als Merkmal weniger geeignet. Am Flughafen Leipzig ist man nach Erprobung anderer Systeme zur Handvenenerkennung übergegangen. Die Lage und Verzweigung der Venen des Handrückens bilden das Erkennungsmerkmal; es erfolgt, auch aus hygienischen Gründen, kein direkter Kontakt mit dem Lesegerät, somit wird auch kein Merkmal hinterlassen, das kopiert werden könnte. Die Venen liegen unter der Haut; ihr Muster ist ohne technische Hilfsmittel nicht auslesbar. Das System basiert auf Verifikation. Die biologischen Daten werden auf den Chip des Mitarbeiterausweises geschrieben und verbleiben damit in der Hand des Besitzers; es gibt keine Datenbank für diese Daten. Zuerst wird die Karte gelesen, dann erfolgt die Präsentation des Handrückens. Aus dem Vergleich mit dem auf der Chipkarte abgespeicherten Template ergibt sich die Zulassung oder Abweisung. Etwa 3.000 Mitarbeiter sind auf diese Weise erfasst. Das System zeichnet sich laut Pieper durch hohe Treffsicherheit selbst bei Verschmutzung der Hand aus und weist nach Herstellerangaben eine FAR von 0,0001% und eine FRR von 0,1% auf.

Zonenbildung. Da Zutrittskontrollsysteme vielfach in die Jahre gekommen, störanfällig, technisch überholt und damit leichter angreifbar geworden sind, werden Überlegungen angestellt, sie durch moderne Systeme zu ersetzen – mit der Tendenz, diese mit Aufgaben zu überfrachten. Hineingepackt werden neben den biometrischen die Personaldaten, Ausweiserstellung, IT-Zugriffe, Zeiterfassung, Kantinenabrechnung und Zutritt zu den Umkleideschränken, Inventarschutz, Besucherabwicklung, Raummanagement bis hin zu Betriebsdatenerfassung und Facility-Management. „Das technisch Machbare ist nicht immer sinnvoll", erläuterte DI Klaus Behling der von zur *Mühlen'schen GmbH*. Zwar gilt es, Synergien zu nutzen. Beispielsweise verfügen Zutrittskontrolle, Einbruchsmeldeanlage und Zeiterfassung über einen gemeinsamen Stammdatensatz als Schnittmenge. Darüber hinaus werden die Systeme schnell zu komplex; Arbeitsgruppen, die eine weitergehende Integration erzielen sollen, werden durch die erforderliche Beiziehung von Experten rasch unübersichtlich.

Handvenenerkennung: Lage und Verzweigung der Venen des Handrückens bilden das Erkennungsmerkmal.

Bei strategischer Vorgangsweise sind anhand einer Risikoanalyse die Ziele zu definieren, nach denen sich die erforderlichen Maßnahmen richten. Zeit- und Raumzonen sind zu bilden, und zwar nach dem „Zwiebelschalenprinzip". An der Geländegrenze und bei Zufahrten können unter Umständen Ausweise mit Barcodes ausreichen. An der Gebäudeaußenhaut sorgen Zutrittskontrollanlagen mit berührungslos arbeitenden Kartenlesern und/oder mit Tastaturen zur PIN-Eingabe für ein erhöhtes Sicherheitsniveau innerhalb des Gebäudes. Als weitere Steigerung könnte der Zutritt zum Rechenzentrum über Fingerprint gesteuert werden, der zum Datenträgerarchiv über 3-D-Gesichtserkennung.

Letztlich brauchen Zutrittsregelungssysteme Menschen, die die Besucher empfangen, Alarme und Störungen bearbeiten, die Systeme verwalten, visuell strategische Zutrittskontrollstellen überwachen und Stichproben nehmen.

Die Einladungen für die Veranstaltungen mit geladenen Gästen wurden mit einem Bar- oder 2D-Code zu versehen, sodass, in Verbindung mit einer Zutrittskontrollanlage, das zeitraubende und personalintensive Abhaken der Einlangenden in Listen entfallen konnte.

Dass und wie biometrische Systeme überlistet werden können, zeigte ein Experte des *Chaos Computer Clubs:* Die Unsicherheit mechanischer Sperrvorrichtungen führten den fast 50 Teilnehmern des Forums der Präsident des *Vereins der Sportsfreunde der Sperrtechnik Deutschland e. V.*, Steffen Wernéry, und Arthur Meister, Gründungsmitglied dieses Vereins, mit praktischen Beispielen vor.

Kurt Hickisch

FOTOS: ARCHIV, PCS SYSTEMTECHNIK GMBH, SOREX