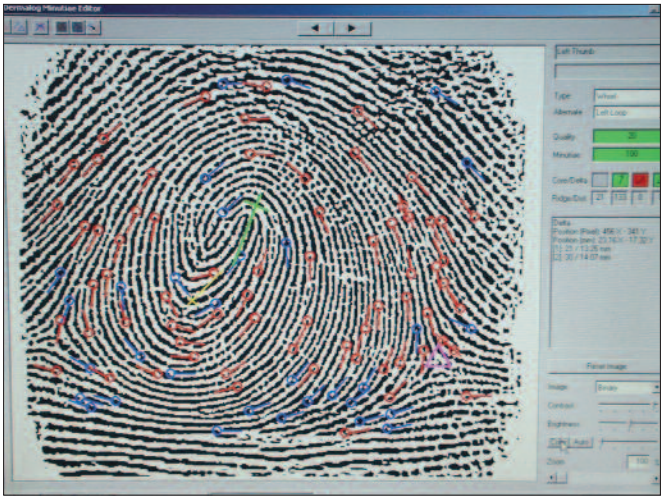
Biometrie: Stärken und Schwächen

Die Anwendung der Biometrie auf Zutrittskontrollsysteme, die Implementierung solcher Systeme und deren praktischer Einsatz waren Hauptthemen einer VfS-Fachtagung in Darmstadt.

Personen können über ihr Wissen um ein Geheimnis authentifiziert werden (Parole, PIN), über den Besitz von Gegenständen (Schlüssel, Magnet- oder Chipkarte, Token), oder auch durch beides zusammen (Zwei-Faktor-Authentifizierung). Wissen kann jedoch vergessen, Besitz verloren werden. Beides kann an andere Personen weitergegeben werden. Eine Personenbindung ist nicht sichergestellt. Charakteristiken des menschlichen Körpers sind hingegen eindeutig. Biometrische Erkennungsverfahren beruhen auf dem Menschen selbst.

Biometrie ist die Vermessung körpereigener Merkmale, definiert als „die automatisierte Erkennung von Individuen anhand deren Verhalten und ihrer biologischen Charakteristika“, erläuterte Alexander Nouak, Abteilungsleiter Identifikation und Biometrie des Fraunhofer-*Instituts für Graphische Datenverarbeitung (IGD)*. Biometrie ist der Forschungsschwerpunkt dieser Abteilung des Fraunhofer IGD in Darmstadt, in dessen Räumen am 11. und 12. Juni 2015 die Fachtagung „Zutritts- und Berechtigungsmanagement“ des *Verbandes für Sicherheitstechnik (VfS; www.vfs-hh.de)* stattfand.

Nouak ging auf Vorurteile ein, die der Anwendung der Biometrie bei Authentifizierungsverfahren entgegenstünden. Biometrie ist – mathematisch nachweisbar – sicherer als die PIN. Die Größe des Informationsgehalts *(Entropie)* liegt bei einer 6-digit-PIN bei 20 bit, beim Gesicht bei 56, beim Fingerabdruck bei 84 und bei der Iriserkennung bei 249 bit. Bei der Gesichtserkennung müssen bei der Registrierung eines Nutzers im System *(Enrolment)* keine Bilder des Gesichts gespeichert werden, sondern bloß extrahierte Datensätze *(Templates)*, aus denen das Originalbild nicht rekonstruiert werden kann. Dabei werden diese Templates, die lediglich die Anordnung bestimmter Referenzpunkte zueinander in Verbindung setzen, in einem Verschlüsselungsprozess zu Pseudonymous Identifiers (PI) transformiert. Durch diese Umwandlung, die nur innerhalb einer Anwendung gleich ist, kann kein Quervergleich *(Cross Matching)* mit anderen Datenbanken erfolgen. Aus aktuell präsentierten Daten werden Templates auf die gleiche Weise erzeugt und mit den abgespeicherten Daten verglichen *(Comparison)*.



Fingerabdruckspeicherung: Biometrische Zutrittskontrollsysteme sind sicherer als PINs.

Laut Nouak sei es für das Enrolment wichtig, auf Qualität zu achten und den Einlernprozess unter Kontrolle zu haben. Nur so könne man die Manipulation des Bildmaterials ausschließen. Bei der Ausstellung von Reisepässen sollte demnach nicht nur die Unterschrift bei der Behörde geleistet, sondern dort auch das Lichtbild aufgenommen und nicht vom Antragsteller mitgebracht werden. Schließlich würden auch die Fingerabdrücke direkt bei der passausstellenden Behörde erhoben.

„Wenn man befürchtet, dass die Gesichtserkennung zu Überwachungszwecken eingesetzt werden könnte – andere Spuren können leichter ausgewertet werden“, trat Nouak einem weiteren Einwand entgegen. Für eine effektive Gesichtserkennung sind gute Beleuchtung, gute Sichtbarkeit des Gesichts und gute Auflösung erforderlich – Bedingungen, die im Alltag nicht leicht zutreffen. Dagegen hinterlässt man digitale Spuren allein schon durch die Nutzung von Mobiltelefonen, die als Feature auch eine Personenüberwachung anbieten. Jede unbare Zahlung hinterlässt Spuren, wo man was gekauft hat.

Vollständig bleibt man Herr über seine Identitätsdaten, wenn diese auf dem mobilen Datenträger selbst gespeichert sind und die Verifikation durch Vergleich mit diesen Daten erfolgt *(Comparison on Card)*.

Über Täuschungsmöglichkeiten beispielsweise gegenüber einem Fingerabdruck-Sensor werde zwar viel berichtet, doch seien die Voraussetzungen (Finger eines Toten) vielfach realitätsfremd. Nicht nur der Fingerabdruck selbst, sondern auch die Fingervenen könnten zur Authentifikation herangezogen werden. Eine andere Möglichkeit liege in der optischen Kohärenztomografie. Bei diesem aus der Medizin kommenden Verfahren, dem im Akustikbereich die Sonografie entspricht, werden beispielsweise auch Schweißdrüsen erfasst.

Die Qualität eines Erkennungssystems ist messbar an Hand der *Falsch-Rückweisungsate (FRR)* gegenüber der *Falsch-Akzeptanzrate (FAR)*. Je höher die Rate der unberechtigten Zurückweisungen ist, umso „unbequemer“ wird das System. Umgekehrt bedeuten fälschliche Akzeptanzen einen Sicherheitsverlust. Auf im Labor ermittelte Werte wird man sich nicht verlassen können. Die entsprechenden Einstellungen müssen empirisch unter den gegebenen Einsatzbedingungen ermittelt werden.

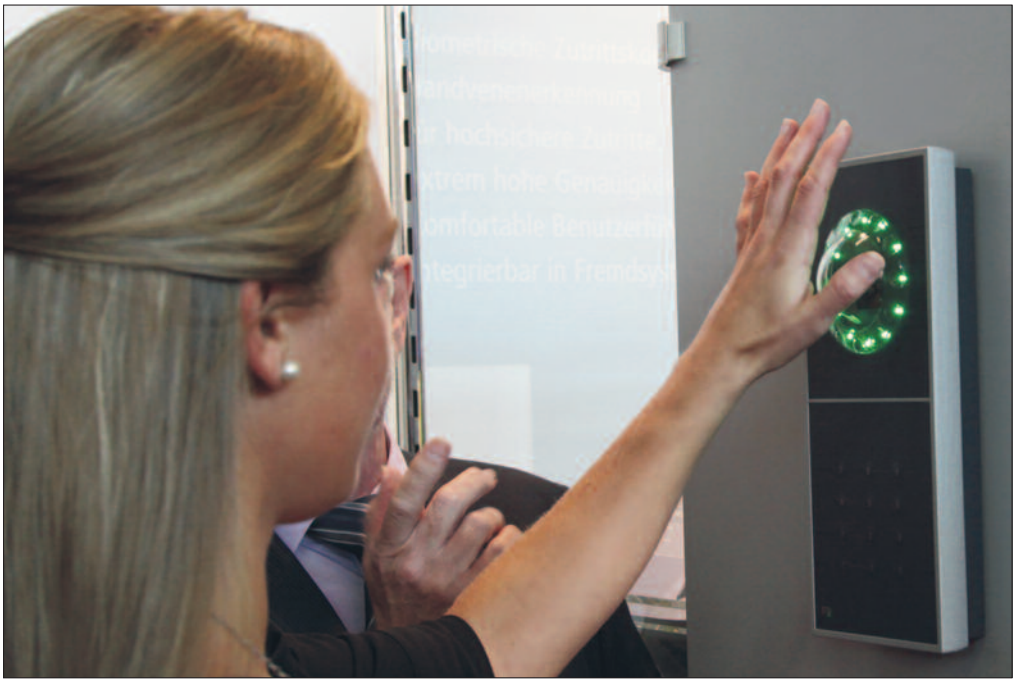
Laut Nouak könnte die Erkennungsrate in der Gesichtserkennung gesteigert werden, wenn auch die Ohren in die Auswertung einbezogen würden. Sensoren könnten fusioniert zusammenwirken: Mikrofone für die Stimmerkennung; Kameras auch für das Erkennen der Lippenbewegung, Be-

FOTO: KURT HICKISCH

schleunigungssensoren im Handy zur Gangerkennung. Tippverhalten und Unterschriftserkennung wären weitere Möglichkeiten, die Genauigkeit einer Authentifizierung zu steigern und „einen Vertrauenstank zu füllen“. Je nach dem Füllstand würden bestimmte Aktionen zugelassen.

Problematiken. Prof. Dr.-Ing. Hasenpusch vom *Ingenieurbüro Rathenow BPS (www.ibr-bps.de)* ging näher auf den Einsatz biometrischer Verfahren in Hochsicherheitsbereichen, vornehmlich im Justizbereich, ein. Neben der Überwindungssicherheit steht dabei auch die juristische Zulässigkeit des Verfahrens im Vordergrund. In einem konkreten Fall wurde dem Fingerabdruckverfahren vor der Handvenenerkennung insofern der Vorzug gegeben, als nur äußerliche biologische Merkmale erfasst werden dürfen, die Handvenen jedoch innen liegen. Ein Zwang, sich biometrischen Verfahren zu unterwerfen, könnte dem Recht auf informationelle Selbstbestimmung entgegenstehen; es müssten Alternativen (herkömmliche Personenkontrolle) zur Verfügung stehen.

Die Erkennung der Retina (Augenhintergrund) würde laut Prof. Dr. Tobias Eggendorfer, Hochschule Ravensburg-Weingarten, Rückschluss auf Erkrankungen zulassen und sei demnach datenschutzrechtlich bedenklich. Dem kopierten Fingerabdruck, dem künstlichen Auge und der künstlichen Hand könnten Lebenderkennung, Temperaturmessung, Durchblutung und kapazitive Merkmale entgegengesetzt werden. Angriffe auf Lesegeräte und Chips seien Angriffe auf Computer und würden als solche nach altbekannten Methoden durchgeführt, wie etwa den „Buffer Overflow“. Dass aus aufgetretenen Fehlern nicht gelernt werde, liege darin, dass die Hersteller von Schließsystemen plötzlich „IT machen“ müssten. Die Kunden würden keine Qualität einfordern, wogegen sich Zusatzsoftware gegen Lücken hervorragend verkaufe. Erkenntnisse der IT-Forensik müssten auf die IT-Sicherheit „rückgekoppelt“ werden.



Handvenenerkennung: Identität einer Person ist eindeutig feststellbar.

FOTO: KURT HICKISCH

Managementsysteme. „Ein Zutritts- und Berechtigungsmanagementsystem sollte weit mehr sein als ein Ausweisverwaltungssystem und alle ausweisbasierten Systeme zusammenfassen“, forderte Volker Kraiss von der *Kraiss&Wilke Security Consult GmbH (www.kraiss-consult.de)*. Die einzelnen Systeme (Zutrittskontrolle, Schließsysteme, Zeiterfassung, Parkmanagement, interne Bezahlsysteme) sollten mit einem multifunktionalen Ausweis so zusammengeführt werden, dass sie herstellerunabhängig unter einer gemeinsamen Bedieneroberfläche verwaltet werden könnten. Das Lastenheft von Ausschreibungen sei mit seinen Anforderungen und Zielsetzungen dementsprechend zu gestalten. Im Pflichtenheft hingegen beschreibt der Auftragnehmer, wie er die im Lastenheft beschriebenen Anforderungen erfüllen will. Dieses wird dann Grundlage des Vertrags. Letztlich kommt es zur Leistungsabnahme, bei der der Grad der Erfüllung der Leistung bewertet wird.

Die Produkte verschiedener Hersteller in ein übergeordnetes Sicherheitsmanagement-System überzuführen, führt zur Schnittstellenproblematik, über die Michael Klitsch von *ensecco (www.ensecco.de)* referierte. Jedes zu integrierende, proprietäre System arbeitet für sich optimal. Bei einer Einbindung in übergeordnete Systeme ist mit einer Funktionseinschränkung zu rechnen, ebenso auch dann, wenn ein System an Standards ausgerichtet werden soll. (Standardisierte) Schnittstellen bilden in der Regel kaum alle Informationen und Funktionen der Subsysteme ab. Normen legen lediglich die Mindesterfordernisse fest. Den Ablauf einer konkreten Umsetzung schilderte Melf Westphal von der *Lufthansa Technik AG* an Hand der Implementierung eines solchen Systems am *LHT*-Betriebsgelände in Hamburg. Im Flughafen-Betriebsgelände sind 10.000 Mitarbeiter beschäftigt. Es ist von einem vier Kilometer langen Zaun umgeben und wird mit 50 Kameras überwacht.

Datenschutz. Helge Carstensen, Personalrat bei *Dataport,* einer Anstalt öffentlichen Rechts, ging auf das Spannungsverhältnis zwischen Sicherheitsmanagement und Datenschutz ein. Damit Zutrittskontrolle nicht zu einer Überwachung der Mitarbeiter führt, dürfe keine Verknüpfung der Zugangsdaten mit Arbeitszeiterfassung (Pausen, Abwesenheiten u. a.) erfolgen, keine Anfertigung von Bewegungsrastern im Gebäude und keine andere automatisierte Verhaltens- und Leistungskontrolle. Für Zugangs- und Zeiterfassungssysteme sollten getrennte Lesegeräte bestehen. Datenauswertung dürfe nur anlassbezogen erfolgen, etwa bei einem Diebstahl, und auch da nur unter

VfS-Fachtagung in Darmstadt zum Thema Zutrittsmanagement: Referenten Alexander Nouak, Andreas Hasenpusch, Tobias Eggendorfer, Volker Kraiss, Wolfgang Schünemann, Wilfried Joswig und Melf Westphal.

Beiziehung des Personalrates nach dem Vier-Augen-Prinzip. Gleiches sei auch für Videoüberwachung zu fordern. Entsprechende Dienstvereinbarungen müssten abgeschlossen werden.

Zur IT-Sicherheit gehört auch, dass bei jedem Verlassen des PC die Bildschirmsperre aktiviert wird. Alle Passwörter dürfen nur eine zeitlich beschränkte Gültigkeitsdauer haben. Zum Wechsel des Passworts ist rechtzeitig automatisiert aufzufordern. Ein Passwortsafe ist bereitzustellen. Hinsichtlich der Gültigkeitszeiträume und der Anforderungen an Länge und Zusammensetzung der Passworte seien die Systeme zu harmonisieren. Bei der Gestaltung von Passwort-Richtlinien sollte der Personalrat mitbestimmen können. Alle Administrator-Aktivitäten sollten über Video protokolliert und aufgezeichnet werden.

Das starke Interesse von Mitarbeitern an der privaten Nutzung mobiler Endgeräte, wie *iPad* und *iPhone*, auch zu dienstlichen Zwecken *(BYOD)* müsste durch entsprechende Vereinbarungen geregelt werden. Auf die Risiken einer solchen Nutzung müsse hingewiesen werden und auch darauf, dass es zu einer Einschränkung der Privatsphäre kommen könnte, falls durch das private Gerät ein Sicherheitsvorfall ausgelöst werde. „Unternehmenskultur statt Sprechblasen" forderte Carstensen. Sicherheit müsse in einem Unternehmen gelebt werden. Statt zu sanktionieren, sei zu sensibilisieren und aufzuklären – was Aufgabe eines „Akzeptanzmanagements" sei. In Sicherheit und Datenschutz sollte investiert werden, anstelle zu sparen. Entsprechende Fortbildung und Qualifizierung seien anzubieten und auszuweiten. Statt hektischer Einführung, die flächendeckendes Chaos produziere, seien eine saubere Prozessanalyse und Verprobungen oder Pilotierungen durchzuführen.

Personalressourcen sollten aufgebaut werden, statt ein halbherziges „Nebenamt" zu etablieren. An die Stelle von Anordnungen sollte frühzeitig eine Einbeziehung der Betroffenen erfolgen. Statt Maßnahmen „durchzudrücken", sollte eine Lösung partnerschaftlich mit Personalrat und den Mitarbeitern erfolgen, mit dem Ziel einer Qualitäts- und Akzeptanzverbesserung. Relevante Unterlagen sollten arbeitsplatzbezogen bereitgestellt werden, etwa durch Verlinkung, anstatt sie irgendwo zu veröffentlichen.

Haftungen. Ein Zutritts- und Berechtigungsmanagement bewegt sich auch im Spannungsfeld zwischen technischen Möglichkeiten und haftungsrechtlichen Herausforderungen, berichtete Prof. Dr. Wolfgang Schünemann *(TU Dortmund)*. So haftet zunächst der Lieferant von Sicherheitstechnik gegenüber dem Unternehmen nach Vertragsrecht für Mängel, aber auch aus Produkthaftung. Derjenige, der Sicherheitstechnik einsetzt, haftet grundsätzlich auch gegenüber dem Aggressor. „Es gibt keine Stand-Your-Ground-Doktrin; der Aggressor ist kein Outlaw", betonte Schürmann. Rechtfertigungsgründe könnten sich aus „Hausrecht", Selbsthilfe und Notwehr/Nothilfe ergeben, aber immer unter dem Gesichtspunkt der Erforderlichkeit. Letztlich haftet der Unternehmer auch gegenüber Dritten, beispielsweise, wenn gegenüber Mitarbeitern und Besuchern Videoüberwachung eingesetzt wird. Hier kommen der Persönlichkeitsschutz und datenschutzrechtliche Bestimmungen zum Tragen.

Von einer Perimetersicherung durch Beleuchtung oder durch akustische Alarmmittel können Immissionen auf Nachbargrundstücke erfolgen, die vom Grundnachbarn nicht geduldet werden müssen – es sei denn, die Immissionen wären unwesentlich (Einhaltung von Grenzwerten) oder ortsüblich (Gewerbebetrieb).

Kurt Hickisch

FRAUNHOFER IGD

Visual Computing

Die *Fraunhofer-Gesellschaft* hat allein in Deutschland 67 Institute mit mehr als 23.000 Mitarbeitern. Sie betreibt anwendungsorientierte Forschung zum unmittelbaren Nutzen für Wirtschaft und Gesellschaft. Das jährliche Budget von rund 2 Milliarden Euro wird zu etwa drei Viertel durch Aufträge aus Industrie und öffentlicher Verwaltung erwirtschaftet. Das *Fraunhofer-Institut für Graphische Datenverarbeitung (Fraunhofer IGD)* ist an seinem Hauptstandort an der TU Darmstadt sowie weiteren Standorten in Rostock, Graz und Singapur und 235 Mitarbeitern die weltweit führende Einrichtung für angewandtes *Visual Computing*. Forschung wird insbesondere betrieben in Richtung Computergrafik und -vision, Mensch-Maschine-Interaktion, (interaktive) Simulationen und Modellbildung. Forschungsschwerpunkte der Abteilung Identifikation und Biometrie sind 3D-Gesichtserkennung, Ohrerkennung, Multibiometrie, Behavior Metrics, Lebend- und Fälschungserkennung, Schutz biometrischer Referenzdaten, Evaluierung und Standardisierung biometrischer Systeme. Die IGD war maßgeblich an der Gründung der *European Association for Biometrics (eab)* beteiligt.

www.igd.fraunhofer.de
www.eab.org

FOTOS: KURT HICKISCH