INTEREST

Datenschutz PRAXIS

Datenschutz – rechtssicher, vollständig, dauerhaft.

Ausgabe Oktober 2005 | 9 € zzgl. MwSt.

Biometrie am Arbeitsplatz

Wenn der Teufel den Beelzebub austreibt ...

Dank der Diskussion über Terrorismusbekämpfung und neue Reisepässe mit RFID ist Biometrie in den Mittelpunkt auch des öffentlichen Interesses gerückt. Wie und wo können im Unternehmen biometrische Verfahren eingesetzt werden? Welchen Nutzen bringen sie, und welche Gefahren sind damit verbunden? Datenschutz PRAXIS zeigt Ihnen, worauf Sie sich einstellen müssen. Vorweg: Sie können beruhigt sein. Denn mit Ihrer Hilfe kann Biometrie auch ein Segen werden.

Unter „Biometrie“ wird im Allgemeinen die Lehre vom Messen und Erfassen der Lebewesen und ihrer Eigenschaften verstanden. Im Zusammenhang mit IT-Sicherheit geht es aber in erster Linie um das Erfassen von personengebundenen Merkmalen, die eine Authentifizierung oder Identifizierung ermöglichen.

Ein Vorteil ist trivial - aber wirksam

Im Gegensatz zu anderen diesbezüglichen Methoden kann man biometrische Merkmale nicht wie ein Passwort vergessen oder wie einen Schlüssel verlieren. Darin liegt ein großer Vorteil.

Voraussetzungen eines biometrischen Merkmals

Damit ein personenbezogenes Merkmal für den Einsatz in Sicherheitsszenarien geeignet ist, muss es einige Vorrausetzungen erfüllen. Es muss

- universell sein, d.h. es muss bei jedem Menschen vorhanden sein. So schließt z.B. ein Spracherkennungssystem alle stummen Menschen aus.
- einzigartig sein, d.h. es darf keine zwei Menschen mit dem gleichen Merkmal geben. Selbst bei eineiigen Zwillingen sind die Fingerabdrücke verschieden.

Inhalt

ISSN-Nr. 1614-6867

Praxishilfen & Muster unter **www.datenschuetzer.de**

- zeitlich unveränderlich sein, d.h. es darf sich im Laufe des Lebens nicht verändern. Gewicht oder Körpergröße (in den ersten 20 Lebensjahren) sind z.B. ungeeignet.
- einfach erfassbar sein, d.h. das Merkmal muss mit preiswerten Sensoren, die sich für die Massenproduktion eignen, gemessen werden können. Eine DNA-Analyse identifiziert einen Menschen mit großer Genauigkeit. Trotzdem ist sie wegen des technischen Aufwandes zur Anmeldung am Arbeitsplatzrechner eher ungeeignet.

Manchen biometrischen Erkennungsmethoden fehlt es an breiter Akzeptanz

Nach diesen Kriterien gibt es einige Verfahren, die heute durchaus für den Einsatz in normalen Unternehmen geeignet erscheinen. Ein Fingerabdruckscanner wird heute in etliche Geräte – von der Maus über den PDA bis zum Notebook – serienmäßig eingebaut. Die Qualität ist allerdings sehr unterschiedlich: Von einfachen, leicht auszutricksenden optischen Sensoren bis zu sog. kapazitiven Sensoren, die lebende von toter Materie unterscheiden können. An manchen haftet ein „Makel“: Das Nehmen des Fingerabdrucks hat beispielsweise das negative Flair der erkennungsdienstlichen Behandlung. Akzeptanz

Der Faktor „Kosten“ unterscheidet die Verfahren maßgeblich

Die Gesichtserkennung – das Standardverfahren bei Ausweisen – wird als kostengünstige Lösung gesehen, da Kameras an Arbeitsplatzrechnern im Zeitalter der Internet-Video-Telefonie zunehmend vorhanden sind. Ebenso ist eine Unterschriftserkennung (im „Papierleben“ weit verbreitet) im Zeitalter von Touch-screens bei PDAs und Tablet-PCs durchaus mit schon vorhandener Hardware möglich.

Demgegenüber ist das Aufnehmen von Iris- oder Retinamustern beim Augen-Scan mit mehr Aufwand verbunden.

Biometrie ist so alt wie der Reisepass. Doch die Gefährdungsszenarien ändern sich ständig

Die bundesdeutschen Reisepässe enthalten von je her biometrische Merkmale: Körpergröße, Foto, Unterschrift und Augenfarbe. Das Foto soll zusätzlich ab Herbst 2005 in einem RFID-Chip auslesbar gespeichert werden. Wirklich neu ist dann ab 2007 die Speicherung des Fingerabdrucks im RFID-Chip. Und dann besteht die Gefahr, dass eine zentrale Datenbank aufgebaut wird, die auch zu anderen Zwecken missbraucht werden kann.

Außerdem haben viele Menschen Angst, dieses Verfahren könnte das Augenlicht gefährden.

Zwei Seiten einer Medaille: Fehlerquote durch „FAR“ und „FRR“

Alle biometrischen Verfahren haben eine Gemeinsamkeit: Zu Beginn werden das Merkmal aufgenommen (Enrollment) und ein Vergleichsdatensatz (Template) erstellt. Je nach natürlicher Variation des Merkmals muss es mehrfach erfasst werden. Denn zwei Unterschriften eines Menschen sind nie wirklich identisch, und Finger werden nie exakt gleich aufgelegt. Mit der Genauigkeit der Erfassung und der Auswertung der Parameter sinkt die Häufigkeit der falschen Akzeptanz (False Acceptance Rate, FAR). Es werden also nur wenige (im Idealfall natürlich keine) Benutzer, ohne das sie berechtigt sind, vom System fälschlich zugelassen.

Sinkt die eine Fehlerquote, steigt automatisch die andere - und umgekehrt. Und das lässt sich nicht ändern.

Mit kleiner werdender FAR steigt leider die Häufigkeit der fälschlichen Abweisung (False Rejection Rate, FRR). Es werden also berechtigte Benutzer vom System fälschlich abgewiesen. Die FAR und die FRR eines Systems können leider nicht unabhängig voneinander

optimiert werden. Ist die eine groß, ist die andere klein und umgekehrt.

Identifizierung heißt nicht automatisch Authentisierung

Außerdem muss zwischen der Identifizierung und der Authentisierung des Nutzers unterschieden werden. Bei der Identifizierung muss das System lediglich aufgrund der hinterlegten Templates den Benutzer zweifelsfrei erkennen. Der Einsatz von Überwachungskameras zum Erkennen von gesuchten Straftätern im öffentlichen Verkehrsraum ist immer eine Identifizierung. Die Identifizierung setzt eine zentral geführte Template-Datenbank voraus.

Relevant für Unternehmen ist v.a. die Authentisierung

Technisch weniger anspruchsvoll ist dagegen die Authentisierung. Der Benutzer gibt seine Identität an, und das System überprüft diese: Durch Eingabe einer Benutzerkennung oder durch Einführen einer Chipkarte sagt der Benutzer dem System, wer er ist; und durch Prüfung biometrischer Merkmale checkt das System die Angaben. Hier ersetzt das biometrische Verfahren im Grunde lediglich die Passworteingabe. Beim typischen Einsatz biometrischer Verfahren im Unternehmen handelt es sich meist um eine Authentisierung.

Der Mensch beeinflusst die Manipulationssicherheit

Die erforderliche Manipulationssicherheit eines Erfassungsgeräts hängt stark vom jeweiligen Anwendungsszenario ab. Muss im Beisein einer geschulten Aufsicht (z.B. Polizeibeamter) der Finger zum Scannen des Fingerabdrucks „aufgelegt“ werden, kann diese viele offensichtliche Manipulationen direkt erkennen und verhindern. Beim Gebäudezutritt oder der Anmeldung am Arbeitsplatzrechner kann z.B. ein Finger oder – und hier liegt ein zentrales Problem – der Fingernachbau beliebig oft unbeobachtet probiert werden. Die technischen Anforderungen an die Manipulationssicherheit sind also viel höher.

Qualitätsmerkmal für den Datenschutz ist der Speicherort

Unter Datenschutzgesichtspunkten ist beim Einsatz von Biometrie v.a. die Frage des Speicherorts der Merkmale wichtig. Die Speicherung kann dezentral sein – z.B. auf einer Chipkarte – oder aber zentral: auf einem Server oder in einer Datenbank. Die zentrale Speicherung weckt Ängste, wenn z.B. bei der Speicherung von Fingerabdrücken zu Authentisierungszwecken eine Datenbank entsteht, die unter Umständen Begehrlichkeiten von Behörden oder – noch schlimmer – Straftätern wecken könnte. Nicht zuletzt deswegen ist die zentrale Speicherung von Merkmalen extrem gefährlich.

Speicherung und Verarbeitung unterliegen hohen Sicherheitsanforderungen

Ein kompromittiertes Passwort kann geändert werden, ein kompromittierter Fingerabdruck dagegen maximal neun Mal. Der Versuch, einen biometrischen Datensatz wie ein statisches Passwort zum Server zwecks Prüfung zu schicken ist also absolut unbrauchbar. Die Kompromittierung der biometrischen Datensätze muss auf jeden Fall verhindert werden. Deshalb dürfen die Speicherung und die Verarbeitung der Merkmale nur in entsprechenden Sicherheitsumgebungen erfolgen.

Auch die dezentrale Speicherung birgt hohe Risiken

Werden die biometrischen Merkmale nur in mobilen Speichergeräten wie Chipkarten und USB-Sticks gespeichert, so verhindert dies den Aufbau einer zentralen Template-Datenbank. Leider besteht dann wieder die Gefahr des Verlierens oder Vergessens des Mediums, was einige Vorteile der biometrischen Verfahren zunichte macht.

Dennoch fördert Biometrie den Datenschutz im Unternehmen

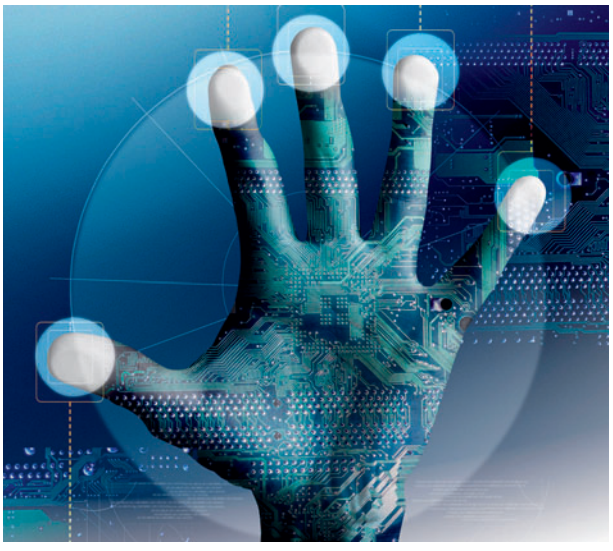
Der große Vorteil der biometrischen Verfahren ist die fehlende Möglichkeit, das Merkmal an andere Nutzer weiterzugeben oder auszuleihen. Auch wenn die Sicherheitspolitik dies im Unternehmen ausdrücklich untersagt, werden Passwörter weitergegeben und manchmal sogar in einem größeren Kreis verabredet.

Biometrie kann dann hilfreich sein, wenn Kollegen die Sensibilität fehlt

Über die Einbeziehung biometrischer Merkmale in die Authentisierung werden Berechtigungen enger an den Nutzer gebunden. Damit wird das „Ausleihen“ eines Passworts während einer Dienstreise unmöglich.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.



Der Scan eines Fingerabdrucks ist die am weitesten verbreitete biometrische Methode.