

ERHOBENER ZEIGEFINGER

Jährlich entstehen weltweit Schäden in Milliardenhöhe durch achtlos aufbewahrte und missbräuchlich verwendete Passwörter. Betriebsgeheimnisse gelangen in fremde Hände, Genehmigungsverfahren werden umgangen und Daten unrechtmäßig manipuliert. Allein für Deutschland schätzen Fachleute, dass die illegale Beschaffung von Daten jährlich einen Schaden von rund 20 Milliarden Euro verursacht. Eine präventive IT-Sicherheitsstrategie ist das Gebot der Stunde.

Laut Ergebnis einer Studie der Gartner Group und des international agierenden IT-Dienstleisters Getronics vom Mai 2005 werden immer mehr Verantwortliche in den Chefetagen die existenzielle Bedeutung der Sicherheit von Informationen für ihr Unternehmen erkennen und entsprechend handeln. Basel II und Sarbanes-Oxley rücken die IT-Sicherheit darüber hinaus noch mehr ins Rampenlicht und zwingen mit ihren verschärften Anforderungen zum Ergreifen präventiver Maßnahmen. Gemäß den Vorgaben der Sarbanes-Oxley-Gesetzgebung zum Thema Informationssicherheit müssen Unternehmen unter anderem dokumentieren, welcher Anwender wann auf welche Daten zugreift.

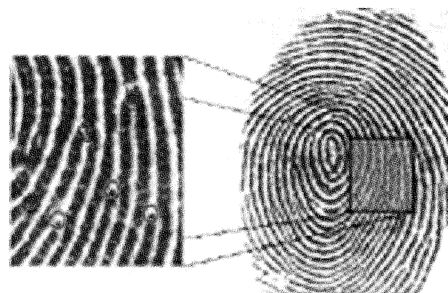
Der Schutz der Informationen – und speziell die IT-Sicherheit – ist heute für jedes Unternehmen eine Grundvoraussetzung für das Geschäft. Doch dieses "must have" alleine reicht nicht aus. Erfolgreiche Unternehmen haben erkannt, dass Informationssicherheit auch ein zentraler Businessbaustein und tragender Pfeiler des Kerngeschäftes ist. Investitionen in diesen Bereich minimieren deutlich das Risiko bei der Einführung neuer Technologien und tragen zur Steigerung der Wettbewerbsfähigkeit bei.

Schließlich beschäftigt sich ein durchschnittlicher PC-Nutzer jährlich rund 44 Stunden mit Anmeldungen per Passwort und ein großer Teil der Computeradministration entfällt auf vergessene Passwörter. Eine weltweite Umfrage von SafeNet bei 2.700 Angestellten im Dezember 2004 bestätigte, dass Mitarbeiter sehr unvorsichtig mit der Zugangskontrolle umgehen. 50 Prozent der Befragten schrei-

ben ihre Codes demnach auf, 35 Prozent tauschen ihre Passwörter untereinander aus, über 80 Prozent haben mindestens drei Schutzbegriffe und 67 Prozent greifen mit einem Passwort auf mindestens fünf Anwendungen zu. Und gut die Hälfte vergisst einmal im Jahr ihre Kombination aus Buchstaben, Zahlen und Zeichen. Dann ist das Helpdesk damit beschäftigt, die Passwörter zurückzusetzen. Die Kosten für diesen Vorgang betragen schätzungsweise 30 bis 50 Euro.

Lösung durch biometrische Authentifizierung

Eine verbesserte Lösung bieten sogenannte biometrische Authentifizierungssysteme. Biometrische Verfahren werden dadurch ermöglicht, dass verschiedene Körper- oder Verhaltensmerkmale eindeutig einem bestimmten Menschen zuzuordnen sind. Erkannt wird der Nutzer hier anhand seiner Individualität. Körperliche Merkmale sind in der Regel untrennbar mit dem Körper der Person ver-



Der Fingerscan weist mit 48 Prozent den größten Marktanteil aller vorhandenen Biometrietekniken auf.



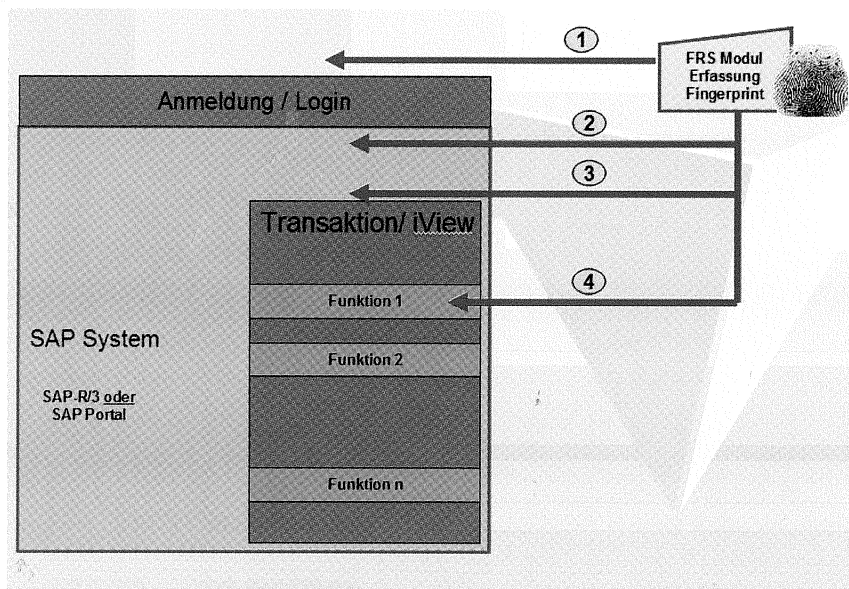
bunden und müssen daher nicht erst dem Berechtigten künstlich zugeordnet werden. Sie können nicht vergessen, weitergegeben, erspäht oder gestohlen werden. Neben der erhöhten Sicherheit ist der gesteigerte Komfort ein weiteres Plus solcher Biometricsysteme.

Biometrische Anwendungsgebiete sind:

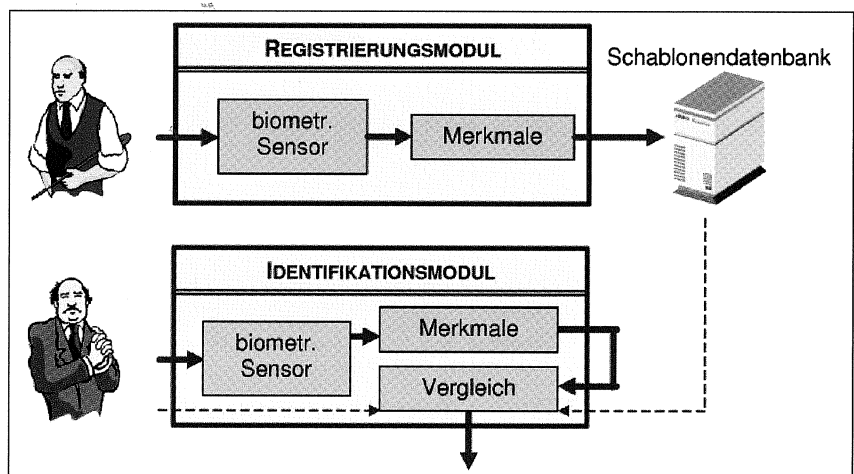
- biometrisch gesicherter und dokumentierter Zutritt zu Gebäuden, Einrichtungen und besonders geschützten Bereichen (z.B. Kassen- und Serverräume, F&E-Abteilungen, Vorstandsetagen, Privatbereiche etc.),
- biometrisch gesicherter und dokumentierter Zugang zu IT-Infrastrukturen (SSO), Systemen und bei weiteren ERP-Systemen über das WWW zum Portal oder direkt in das firmeneigene Intranet, bei der Zeiterfassung und den personenbezogenen Daten im HR-Umfeld zu Kioskanwendungen,
- biometrisch gesicherte und dokumentierte Freigabe von Transaktionsaufruf und Bestätigungen im SAP-Systemumfeld von Prozessen und sensiblen, operativen Abläufen von Transaktionsbestätigung auf vorhandenen Internetportalen (Bank, Shop etc.) zum Dokumentenschutz.

Fingerprint - das meistverbreitete Authentifizierungssystem

Der Gesamtmarkt für biometrische Erkennungsprodukte teilt sich in sechs Technologiebereiche auf. Dies sind Technologien, die Finger, Gesicht, Hand, Iris, Stimme oder die Unterschrift als Authentifizierungsmerkmal benutzen. Der Weltmarkt teilt sich zu rund 71 Prozent in drei führende Technologien (Fingerscan, Gesichtsscan, Handscan) auf, wobei der Fingerscan mit 48 Prozent den größten Marktanteil aller vorhandenen Biometrie-techniken inne hat. Dies bedeutet aber nicht, dass die anderen Technologien qualitativ schlechter sind. Vielmehr haben sich die jeweiligen Systemanbieter auf die drei führenden Technologien bei der Vorauswahl der Hardware festgelegt. Von allen biometrischen Systemen hat sich die Fingerabdruckererkennung als das universellste Verfahren durchgesetzt. Mit Hilfe einer biometrischen Authentifizierung über den eindeutigen Fingerabdruck der Anwender lässt sich die Sicherheit von Daten in allen Bereichen wesentlich erhöhen. Der Anwender meldet



Anmeldung bei einem SAP-System mit der Fingerprint-Methode



Allgemeines biometrisches System

sich lediglich durch seinen Fingerabdruck im System an und bekommt danach alle für ihn vorgesehenen Rechte zugeordnet. Zusätzlich können sensible Funktionen und Informationen innerhalb der Systeme durch den Fingerabdruck abgesichert werden. Dieses Verfahren bietet hohe Sicherheit und Akzeptanz durch die Benutzer. Die auf dem Markt bereits vorhandenen Systeme sind ausgereift und arbeiten seit Jahren zur vollen Zufriedenheit ihrer Anwender. Biometrische Authentifizierung durch den Fingerabdruck stellt sicher, dass nur die Personen Zugang zu Systemen, sensiblen Funktionen und Informationen bekommen, die sich durch ihren eindeutigen Fingerabdruck identifizieren und somit ausweisen können. Datenmissbrauch, der häufig durch achtlos verwahrte Passwörter betrieben werden kann, findet nicht mehr statt. Hinzu kommt die deutliche Reduzierung der

Kosten für die Systemadministration durch weniger Aufwand in der Passwortverwaltung.

Authentifizierung im SAP-System

Bei der Einführung von biometrischen Verfahren ist es aus betrieblicher Sicht notwendig, sicherheitsrelevante Bereiche zunächst in ihrer Gesamtheit zu identifizieren und dies bei der Auswahl entsprechender technischer Lösungen zu berücksichtigen. Mit anderen Worten, die selektierte technische Lösung sollte weitgehend modular aufgebaut, die Erfassung und Verarbeitung biometrischer Daten unabhängig von ihrer Verwendung sein und unterschiedlichsten Sicherheitsanforderungen gerecht werden. Ein Beispiel: Die von it-motive zusammen mit Partnern entwickelte Lösung "SecID" sieht eine beliebig skalierbare Realisierung von verschiedenen Sicherheitsstufen vor:



- Vor der Anmeldung ins System (Single Sign On)
- Nach der Anmeldung (z.B. im ERP-System)
- Vor dem Start der Transaktion/ Menü/iView
- Innerhalb einer Funktion: Button, Save, Freigabe etc.

SecID wird nahtlos ins SAP-System integriert. Dies bietet weitreichende Vorteile: So erfolgt kein Eingriff in das SAP-Berechtigungskonzept, das SAP-Berechtigungskonzept bleibt von der biometrischen Authentifizierung unberührt. Das System stellt sicher, dass Funktionen (Anmeldung, Aufruf von Transaktionen etc.) tatsächlich von der Person ausgeführt werden, die im SAP-System angemeldet ist und laut Berech-

tigungskonzept zur Ausführung berechtigt ist.

Bei einer Authentifizierung auf Funktions- und Feldebene stellt SecID eine Erweiterung zum Berechtigungskonzept (unabhängig vom SAP-Berechtigungskonzept) dar. Im Einzelfall muss entsprechend der Anforderungen geprüft werden, wie über die im SAP-System vorhandene Exit-Technik eine Authentifizierung aufgerufen werden kann.

Biometrische IT-Projekte erfordern umfassende Evaluierung

Die Integration und Verwendung ökonomisch effizienter, akzeptierter und funktionaler Biometricapplikationen erfordern die Beachtung einer Vielzahl von Komponenten wie z.B. der Nutzergruppe, bestehender IT-Struktur, Ergonomie, physika-

lischer Rahmenbedingungen wie Temperaturbeständigkeit usw. Unternehmen mit langjähriger Biometrieerfahrung unterstützen private Unternehmen und staatliche Organisationen bei der Umsetzung von biometrischen IT-Projekten. Das Spektrum der Dienstleistung reicht von der Ideenfindung, Analyse und Konzepterstellung bis zur operativen Umsetzung im Unternehmen. Doch der wichtigste Schritt ist – wie bei allen IT-Projekten – die Evaluierung des eigenen Bedarfs und die Erstellung eines umfassenden Anforderungsprofils. (ap) @

it-motive

Tel.: (0203) 60878-0

Fax: (0203) 60878-222

E-Mail: info@it-motive.de

Internet: www.it-motive.de

MASSGESCHNEIDERTE PUBLIC-KEY-INFRASTRUKTUREN

SICHER, VERSCHLÜSSELT UND BENUTZERFREUNDLICH

Der Bedarf an Sicherheit wächst, die Anforderungen steigen. Aufgrund der Entwicklung der vergangenen Jahre erlangt der Schutz firmeninterner Daten für Unternehmen zunehmende Bedeutung. Verschlüsselungen und Verschlüsselungssoftware sind gefragt wie nie zuvor.

VON ALEXANDER KERWIEN*

Die von den meisten größeren Unternehmen eingesetzte betriebswirtschaftliche Standardsoftware der SAP bietet mit der SNC-Schnittstelle zwar eine Schnittstelle für Kryptosoftware, SAP selbst bietet jedoch keine eigene Lösung zur Verschlüsselung zwischen Client und Server an. Dieser Markt wird stattdessen von Drittanbietern bedient. Unternehmen mit SAP-Systemen stehen somit vor der Herausforderung, aus den Produkten einer Handvoll Anbieter das Geeignete auszuwählen. Häufigstes Problem hierbei sind die vielen, teils sehr individuellen Anforderungen, welche die Software erfüllen soll. Diesen berechtigten Ansprü-

chen kann eine Software von der Stange meist nicht nachkommen. Deshalb bieten verschiedene IT-Spezialisten maßgeschneiderte Sicherheitslösungen für Unternehmen, die SAP-Systeme einsetzen, an.

Unternehmen, die ihre bereits vorhandene Software ihren steigenden Sicherheitsbedürfnissen anpassen möchten, stehen vor der Aufgabe, zunächst ein Anforderungsprofil zu erstellen. Zu den am häufigsten genannten Anforderungen an die Sicherheitslösung zählt die verschlüsselte Übertragung von Passwörtern und Anwendungsdaten beim Arbeiten mit SAP-Systemen. Über die Sicherheit des Systems hinaus sind für einen Großteil der Unternehmen leichte Bedienbarkeit, geringer Schulungsaufwand, einfache Admi-

nistrierbarkeit durch die interne Administration, kein zusätzlicher Wartungsaufwand und Kompatibilität mit weiteren, hausinternen Anwendungen von erheblicher Bedeutung.

Trotz ähnlicher Bedürfnisse und Vorstellungen, gibt es in der Regel keine Standardsoftware, die all diese Anforderungen "Out of the Box" erfüllt. Stattdessen kombinieren die beauftragten IT-Unternehmen verschiedene Produkte miteinander und passen sie in die bestehende Systemlandschaft ein.

Um Lösungsansatz, Umsetzung und Kostenrahmen konkret zu fassen, kann ein in der Praxis gängiger Auftrag als Beispiel dienen: Ein mittelständisches Unternehmen mit SAP-Systemlandschaft (beispielsweise "SAP R/3" und "SAP Business Warehouse") und 300 Anwendern

*Alexander Kerwien ist Senior Security Consultant bei der SecurIntegration GmbH