IT-SICHERHEIT

Neue Risiken

Mobile Computing, Biometrie und E-Government waren Schwerpunktthemen beim 2. Darmstädter Sicherheitstag.

Mobile Computing ist die Nutzung mobiler Geräte und mobiler Netze und ermöglicht, jederzeit und örtlich ungebunden auf benötigte Informationen (M-Commerce, M-Business) und Daten zurückzugreifen, etwa als Außendienstmitarbeiter, der Kundendaten, als Prüfingenieur, der Handbücher abrufen oder als Arzt, der unmittelbar beim Kranken oder dem Unfallopfer Daten einholen kann.

Arbeit wird nicht mehr an einen festen Arbeitsplatz gebunden sein, wenn auf E-Mails und Unternehmensdaten von überall her rund um die Uhr zurückgegriffen werden kann. Die Effektivität der Arbeit wird, unter anderem durch verkürzte Bearbeitungszeiten erhöht, und auch die Qualität wird gesteigert (keine Medienbrüche oder Übertragungsfehler). Allerdings kommen zu den bekannten Sicherheitsproblemen (Computerviren, -würmer, Trojaner, Mailbomben) neue Risiken dazu, berichtete Prof. Dr. Claudia Eckert bei dem vom Fraunhofer-Institut für Sichere Telekooperation (SIT) veranstalteten Sicherheitstag. Die mobilen Geräte sind klein und werden leicht vergessen und liegen gelassen und können leicht gestohlen werden.

In Londoner Taxen wurden im ersten Halbjahr 2001 2.900 Laptops, 1.300 PDAs und 62.000 Mobiltelefone zurückgelassen. Dazu kommt, dass in die kleinen Geräte mit ihren knappen Ressourcen (geringerer Speicherplatz, begrenzte Batterieleistung) nicht jener Sicherheitsstandard erreicht werden kann, wie er bei stationären Geräten üblich ist.

Die Geräte werden oft an Orten mit hoher Kommunikationsdichte (Bahnhöfe, Flughäfen) betrieben, wo „Hot Spots“ eingerichtet sind. Das verstärkt die durch die Nutzung von Funkverbindungen ohnehin schon gegebene Unsicherheit vor „Abhören“.

„Mobiles Arbeiten wird unaufhaltsam kommen,“ erläuterte Eckert, „aber Mobile Security muss in die Unternehmensstrategie eingeplant werden.“

Biometrische Verfahren werden auf den Flughäfen Schipol, Amsterdam, und Kingsford Smith, Sidney, Australien eingesetzt. Fluggäste, die sich dem biometrischen Verfahren (Iriserkennung) unterziehen, werden beim Grenzübertritt rascher abgefertigt. Sie haben eine Smartcard, auf der die mit einem Algorithmus umgewandelten Daten kryptografisch festgehalten sind. Bei einer fälschlichen Zurückweisung, einem „Fallback-Szenario“, wird wie gewohnt manuell kontrolliert.

Durch Gesichts- und Iriserkennung kann erkannt werden, ob Personen berechtigt sind, das Cockpit betreten und ob sie später das Flugzeug auch steuern. Ist das nicht der Fall, übernimmt der Autopilot die Steuerung und landet das Luftfahrzeug.

Angriffspunkte für biometrische Verfahren sind der Sensor, der getäuscht werden kann, und die Datenübertragung und -speicherung. Der Vorteil liegt darin, dass man biometrische Merkmale immer bei sich hat, sie also nicht vergessen, verlieren oder weitergeben kann.

Öffentliche Sicherheit, Ausgabe 03-04/2003

Zusätzliche Sicherheit bedeutet zusätzlichen Aufwand; letztlich ist dieser dem Ausmaß der zu fordernden Überwindungssicherheit gegenüberzustellen.

Bei der „digitalen Signatur“ gibt es noch keinen Durchbruch. Ursache ist, dass es noch zu keiner universellen Nutzbarkeit einer Signaturkarte gekommen ist, dass mit ihr nicht nur digitale Schriftstücke autorisiert, sondern auch Zahlungsvorgänge, Banktransaktionen oder etwa das Lösen eines Fahrscheins erledigt werden können.

Kurt Hickisch

Fraunhofer-Institut für Sichere Telekooperation (SIT), http://www.sit.fraunhofer.de/