

Geschrieben, gespeichert, geklaut?

Dass wichtige Firmendaten auf mobilen Geräten liegen, ist längst Alltag. Doch die kleinen Helfer gehen leicht verloren oder werden gestohlen. Richtiges Verhalten und Sicherheitstools minimieren das Risiko.

Nicht jeder Mittelständler speichert auf seinem Notebook so hochgeheime Daten wie jener britische Geheimdienstler, dem sein zwischen den Beinen abgestellter Laptop mit Nordirland-Informationen geklaut wurde, als er in der U-Bahnstation nach Kleingeld suchte. Trotzdem gilt besonders für Unternehmer: „Egal, ob ein Gerät gestohlen wird oder verloren geht – die Vorstellung, dass Fremde in den eigenen Daten wühlen, ist immer unangenehm“, weiß Ansgar Heinen, Datensicherheitsexperte bei der Utimaco Safeware AG in Oberursel. Eine Umfrage seines Unternehmens unter den Fundbüros der zehn größten Flughäfen in Deutschland, Österreich und der Schweiz ergab, dass Reisende dort im vergangenen Jahr mehr als 5.000 mobile Geräte verloren hatten. Meistens vergaßen ihre Besitzer ganz einfach, ihre Handys und PDA nach den Sicherheitskontrollen wieder einzupacken. Bei immerhin einem Viertel aller Fälle meldeten sich die Besitzer nicht einmal innerhalb einer Woche, so die Fundbüromitarbeiter.

Politikum Sicherheit. Der erste Schritt, um die IT-Sicherheit zu erhöhen, ist eine Bestandsaufnahme. In den meisten Firmen ist unbekannt, auf welchen mobilen Geräten Unternehmensdaten gespeichert werden. Vielerorts werden Daten von Firmencomputern auf privaten Geräten kopiert, ohne dass die IT-Administratoren davon wissen. Besonders gilt dies für den Termin- und Adressabgleich zwischen Outlook am Arbeitsplatz und dem PDA. „Als ersten Schritt gilt es, den Wildwuchs zu stoppen“, fordert Jürgen Borchert, Geschäftsführer des Software-Anbieters Pointsec in Düsseldorf. Daher lautet die wichtigste Regel, noch bevor etwas verloren geht oder gestohlen wurde: Private PDA dürfen nicht an das Firmennetzwerk angeschlossen werden. Hier taucht schon das erste Problem auf, denn oft ist der Betriebsrat schon mit der eingeschränkten Nutzung des Internets oder dem Verbot privater E-Mails nicht einverstanden. Das Verbot der Synchronisierung wird als weitere Gängelung empfunden. „Besonders in mittelgroßen Betrieben wird diese Grundvoraussetzung für effektiven Datenschutz zu einer politisch heiklen Angelegenheit“, so Borcherts Erfahrung. Um solche Fallstricke zu umgehen, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) allen Firmen, die Mitarbeiter nicht nur über die Vorteile, sondern auch über die mit dem Einsatz mobiler Endgeräte verbundenen Gefahren aufzuklären und schriftlich festzulegen, was erlaubt ist und was nicht.

Verboten werden sollte übrigens auch das Synchronisieren des Firmen-PDA mit dem privaten PC, weil dadurch Schadsoftware wie Viren und Trojaner in das Firmennetz eingeschleppt werden kann. Unter allen Umständen muss schriftlich geregelt sein, wie häufig und bei welchen Anlässen Daten von PDA, Notebooks oder anderen Speichermedien zu sichern sind. Denn sowohl Festplatten als auch Flash-Speicher sind anfällig für mechanische Fehler, wenn sie herumgetragen, im Kofferraum durchgeschüttelt oder sogar fallen gelassen werden.

Daten verschlüsseln. Auf Notebooks mit großen Festplatten finden sich oft nicht nur viele heikle Dokumente, sondern auch der Fernzugang zum Firmennetzwerk und die dafür notwendigen Passwörter. Ein erster Schritt ist es, den Zugang zum Gerät selbst mit einem Passwort zu schützen. Doch diese Sperre umgehen Profis leicht, vor allem wenn die Passwörter zu einfach gewählt sind. Eine bessere Alternative sind Hardware-Lösungen wie Smartcards oder Token. Letztere haben den Vorteil, ohne Lesegerät auszukommen, weil sie direkt in den USB-Port gesteckt werden. Der User tippt zunächst seine PIN ein. Daraus errechnet der Token mithilfe des auf seinem Mikrochip hinterlegten Algorithmus eine einmalige Zahlenkombination, nach deren Eingabe der Zugriff auf das Notebook freigegeben wird. Anders als ein auf

dem Laptop dauerhaft hinterlegtes Passwort oder vierstellige PIN ist ein solcher Code nur mit erheblichem Rechenaufwand zu knacken. Bei diesem Verfahren werden auch die Daten selbst verschlüsselt – entweder nur ausgewählte Dateien oder aber die komplette Festplatte. Das ist wichtig, damit auch jene Informationen, die von Windows in eine temporäre Datei ausgelagert wurden, vor fremden Blicken geschützt bleiben. Die Daten werden bei Bedarf entschlüsselt, in den Arbeitsspeicher geladen und beim Schreiben automatisch wieder verschlüsselt gesichert, wobei der Nutzer dies kaum registriert, weil sich die Reaktionen auf seine Eingaben allenfalls leicht verzögern. Auf dem Markt sind ein Dutzend solcher Lösungen erhältlich, die sich jedoch bei Support und Preisen stark unterscheiden.

Während es für die Verschlüsselung von Notebooks zahlreiche Produkte gibt, dünnt sich das Feld der Anbieter bei der Verschlüsselung von kleineren Geräten schon erheblich aus. Die meisten Anbieter haben Produkte für PDA, MDA, Smartphones und USB-Sticks sowie Speicherkarten im Programm. Für ihren Schutz wird die Software-Lösung auf einen vorhandenen Server aufgespielt. Wird ein Endgerät an einen PC im Netzwerk angeschlossen, installiert das System automatisch die Verschlüsselungssoftware. Der Nutzer wird aufgefordert, ein Passwort festzulegen, mit dem er seine Daten entsperren kann. Danach verschlüsselt das System im Hintergrund die Daten. Dazu muss das mobile Gerät nicht weiter am Netzwerk angeschlossen bleiben. Bei manchen Lösungen kann man es sogar zwischenzeitlich ausschalten, der Verschlüsselungsprozess geht beim nächsten Start nahtlos weiter. Die Verschlüsselungslösung sollte möglichst eng in das vorhandene Sicherheitskonzept eingebunden werden, damit sie nicht neue Einfallstore für Angriffe aufreißt. Wer bereits Smartcards oder Token für die Arbeitsplatzrechner einsetzt, sollte sichergehen, dass die Verschlüsselungslösung für die mobilen Geräte das gleiche Niveau an Sicherheit bietet. Es hilft wenig, die PCs mit einer Zwei-Faktor-Authentifizierung abzusichern, bei der der Nutzer gleichzeitig seine PIN und einen vom Token generierten Zufallscode eingeben muss, wenn sein Notebook und PDA nur mittels vierstelliger Zahlenkombination geschützt sind.

Alle Hersteller rühmen sich damit, dass ihre Lösungen die kleinen Geräte nicht ausbremsen. Zu den Anbietern zählen unter anderem Utimaco, Secude, Safeboot und Pointsec. Safeboot beispielsweise verspricht Leistungseinbußen von maximal 1,8 Prozent, wenn man einen sehr sicheren 256bit-langen Schlüssel verwendet. Die Preise sind ähnlich: Ab 100 Nutzern berechnet Pointsec 120 Euro pro Notebook, Safeboot nimmt 110 Euro, bei beiden ist eine Management-Konsole inklusive.

Wie jeder seinen PDA schützen kann

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät jedem PDA-Besitzer, die Sicherheitsmechanismen des Geräts zu nutzen, solange keine zusätzlichen Tools installiert sind:

- > **Bedienungsanleitung** sorgfältig auf alle möglichen Zugangsbeschränkungen prüfen
- > **Passwortschutz** aktivieren
- > Angemessen komplexe und lange **Passwörter** wählen
- > **Automatische Sperre** einschalten, die sich nach Arbeitsunterbrechungen selbst aktiviert. Die Zeitspanne sollte maximal fünf Minuten betragen.
- > Nach dem Einschalten des PDA sollten **Kontaktdaten des Besitzers** erscheinen, damit sich der ehrliche Finder bei ihm melden kann. Keinesfalls die private Wohnadresse angeben, damit nicht Kriminelle den Anstoß zu einem Einbruch erhalten, besonders wenn im Kalender auch noch die Abwesenheitszeit angegeben ist!
- > Eventuell mitgelieferte **Verschlüsselungsfunktion** für besonders vertrauliche Daten nutzen.

Was tun bei Handy-Verlust?

Gehen Blackberry oder Communicator trotz aller Vorsichtsmaßnahmen verloren, muss der Eigentümer schnell handeln. **Als erstes** sollte der Besitzer seinen Netzbetreiber über die Hotline anrufen und die SIM-Karte sperren lassen, damit

niemand auf seine Kosten telefonieren kann. Über die IMEI-Nummer (International Mobile Equipment Identifier) lässt sich jedes Handy genau identifizieren. Wer Rechnung oder Service-Unterlagen seines Mobiltelefons nicht mehr hat, kann die IMEI mit der Tastenkombination „*#06#“ aufrufen.

Auf Wunsch registriert die Polizei diese Nummer und stellt einen Handy-Pass aus. Sobald gestohlene Mobiltelefone am Markt auftauchen, werden ihre IMEI-Nummern mit den Verlustlisten verglichen. Das gilt auch für die Seriennummern anderer mobiler Geräte. Vodafone bietet seinen Kunden an, im Verlustfall nicht nur die Karte per Funksignal zu sperren, sondern auch das Handy selbst.

ProFirma PREMIUM

Checkliste Datensicherung

Das regelmäßige Sichern ist einer der wichtigsten Teilbereiche der IT-Security. Die Checklisten zeigen Schritt für Schritt die Sicherungsziele sowie den Umfang der Datensicherung auf.

Einfach auf ProFirma.de im Suchfeld „Checkliste Datensicherung“ eingeben und das Tool aus der Trefferliste auswählen.

Autoren: Nicola D. Schmidt und Elmar Török

Ausgabe: 10/2006

<http://www.profirma.de>

© HAUFE MEDIENGRUPPE 2006