

**W**enn Heiko Biesterfeldt abends sein Büro in der Hamburger Speicherstadt verlässt, steckt er immer eine kleine Metallbox ein: eine mobile Festplatte. »Darauf ist stets der aktuelle Datenbestand meiner Agentur gespeichert«, erklärt der Chef der Ad Publica Public Relations GmbH. Übertrieben findet Biesterfeldt diese Vorsichtsmaßnahme nicht: »Vor drei Jahren haben wir bei einem Computercrash quasi über Nacht fast alle Firmendaten verloren – seither gehe ich lieber auf Nummer sicher.«

Nahezu jedes Unternehmen kennt solche oder ähnliche Katastrophen: Rechner geben ihren Geist auf und nehmen wichtige Firmendaten mit ins Nirwana. Handys werden gestohlen, Laptops bleiben im ICE liegen und heimtückische Viren legen ganze Unternehmensnetzwerke lahm. Umso erstaunlicher ist, was das Beratungshaus Steria Mummert Consulting jetzt herausgefunden hat: Nur die Hälfte der Unternehmen ist auf solche Notfälle wirklich gut vorbereitet.

### **Insolvent nach Datenverlust**

Dabei ist Prävention kein Hexenwerk. Was im akuten Fall zu tun ist, wenn etwa das Mobiltelefon abhanden kommt, zeigt die Checkliste (siehe »Handy vermisst«). Online unter [www.impulse.de/it-strategien](http://www.impulse.de/it-strategien) finden sich zudem ausführliche Tipps, wie Firmenchefs vorgehen können, um sich vor den größten IT-Risiken zu schützen. Denn der Datenverlust hat oft dramatische Folgen. Gehen Buchhaltungs- und Konstruktionsdaten, Kundenadressen und Lagerbestände verloren, führt das nach einer

Untersuchung der Meta Group bei immerhin 60 Prozent der betroffenen Unternehmen in den Konkurs.

Zu den am meisten gefürchteten IT-Notfällen gehört der Virenbefall. Die digitalen Schädlinge verursachen nach Angabe des Bundesamts für Sicherheit in der Informationstechnik (BSI) allein in Deutschland jährlich

Schäden in dreistelliger Millionenhöhe. Die größte Gefahr geht dabei von boshafte Programmen aus, die heimlich wichtige Dateien löschen oder Firmengeheimnisse ausspionieren. Schlimm sind aber auch die Panikreaktionen unerfahrener Anwender, wenn sie merken, dass ein Virus den Bürorechner infiziert hat. Um das Schadprogramm zu eliminieren, installieren sie oft das Betriebssystem neu und überschreiben damit die komplette Festplatte. Sämtliche Programme und Daten sind perdu, sofern sie nicht im Firmenarchiv als Duplikat gespeichert wurden.

Für den Notfall geben Firmenchefs am besten eine klare Direktive aus: Besteht bei einem Büro-PC der Verdacht auf Virenfektion, sollte der Computer umgehend vom Firmennetz getrennt werden. »Damit kann das infizierte Gerät keine weiteren Rechner mehr anstecken«, erklärt Olaf Lindner vom Anti-Viren-Spezialisten Symantec. Anschließend lässt sich dann mithilfe von Schutzsoftware feststellen, ob tatsächlich

Gefahr besteht. Manchmal registrieren Anti-Viren-Programme zwar ungewöhnliche Aktivitäten auf der Festplatte, dahinter kann aber auch ein harmloser Programmfehler stecken.

### **Mobiles Risiko**

Lässt sich die IT innerhalb der Firma noch sehr gut schützen, so herrschen außerhalb des Büros andere Bedingungen: Allein mehr als fünf Millionen Handy-Nutzer in Deutschland sind bereits Opfer von Diebstahl geworden und haben ihr Mobiltelefon nie wiedergesehen. Höchstens auf Auktionsplattformen im Internet, wo Langfinger Telefone, PCs und Notebooks massenhaft anbieten sollen. Sogar ausgebaute Computerfestplatten, voll mit sensiblen Firmendaten, tauchen regelmäßig bei Online-Händlern auf.

Durch den Einsatz von Mobilgeräten wie Laptops oder Blackberrys machen sich Unternehmen beson-

# Erste Hilfe

Handys gehen verloren, Rechner stürzen ab, Laptops werden gestohlen. Wie sich Unternehmer auf Notfälle vorbereiten.

ders angreifbar: Denn 40 Prozent der Firmen, so die Steria-Mummert-Studie, unterschätzen die Gefahr und sind nach wie vor nicht ausreichend gegen unbefugte Zugriffe gesichert. Der Verlust mobiler Rechner ist besonders dramatisch, weil sich mit diesen oft eine direkte Verbindung in das Firmennetzwerk aufbauen lässt.

Agenturchef Biesterfeldt hat für die Vogel-Strauß-Politik vieler seiner Unternehmern Kollegen kein Verständnis: Seit dem Totalausfall vor drei Jahren legt er größten Wert auf eine optimale Notfallplanung. Nicht nur, dass er die kompletten Firmendaten täglich mit nach Hause nimmt. Zusätzlich hat der Hanseat auch die Zahl der Server, über die alle Daten laufen, auf vier verdoppelt und ein besonders ausfallsicheres Speichersystem installiert. Außerdem sicherte er sich die Dienste von Spezialisten: Bevor er oder ein Mitarbeiter im Notfall etwas falsch machen, ruft er lieber die Profis. »Wir haben einen Wartungsvertrag mit der PC-Feuerwehr Hamburg-Mitte GmbH geschlossen«, erklärt Biesterfeldt. Die IT-Experten stehen Gewähr bei Fuß, wenn die Firmendaten in Gefahr sind – und das 24 Stunden am Tag.

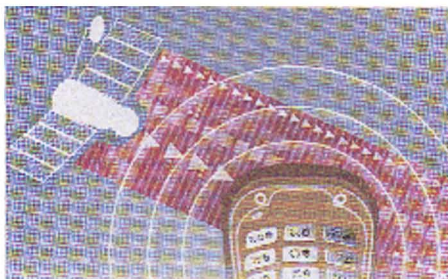
Manfred Buchner [ressort.computer@impulse.de](mailto:ressort.computer@impulse.de)

## **WWW. | [impulse.de](http://impulse.de)**

**/it-strategien** Die impulse-Checklisten für den Notfall: So schützen Sie Ihre Computer und Netzwerke. Hier finden Sie konkrete Ratschläge, wie Sie in Notsituationen vorgehen sollten, um Schäden zu minimieren. Wenn Viren den PC lahmlegen, das Notebook gestohlen wurde oder die komplette Firmen-IT ausfällt. Profitieren Sie von Erste-Hilfe-Plänen, kurz und übersichtlich formuliert, zum Ausdrucken und Mitnehmen.

## **Handy vermisst**

Was tun, wenn das Mobiltelefon spurlos verschwunden ist? impulse zeigt die vier wichtigsten Schritte.



### **1 | Wählen Sie die eigene Rufnummer.**

Klingt trivial, führt aber oft zum Erfolg: Entweder bimmelt das Gerät unter einem Stapel Papier oder es meldet sich der ehrliche Finder.

### **2 | Ist das Handy per Anruf nicht aufzuspüren, sperren Sie die Telefonkarte beim Service-Provider. Damit vermeiden Sie, dass Unbefugte auf Ihre Kosten telefonieren.**

#### **Die wichtigsten Hotline-Nummern:**

T-Mobile (D1) +49 (0) 1803-302202

Vodafone (D2) +49 (0) 800-1721212

E-Plus +49 (0) 177-100002

O<sub>2</sub> +49 (0) 1805-624357

### **3 | Melden Sie den Verlust** des Mobiltelefons beim Fundbüro. Zum Beispiel im Internet unter → [www.fundbuero24.de](http://www.fundbuero24.de) oder → [www.fundservice.bahn.de](http://www.fundservice.bahn.de)

### **4 | Sie können das Gerät auch komplett sperren lassen, damit Unbefugte es nicht nutzen. Hierfür benötigen Sie die sogenannte IMEI(International Mobile Equipment Identity)-Nummer. Anhand dieses 15-stelligen Codes kann jedes Handy eindeutig identifiziert und beim nächsten Einwählen ins Mobilfunknetz gesperrt werden. Die Nummer befindet sich in der Regel auf dem Typenschild. Dieses wiederum klebt meist unterhalb des Handy-Akkus. Tipp:** Vor dem ersten Einsatz den Aufkleber entfernen und an einem sicheren Ort verwahren, damit Sie den Code immer griffbereit haben.