## IT-SOFTWARE

### Weltweites Backup
Novastor hat die zehnte Auflage von Novabackup lanciert. Sie erlaubt es den Anwendern, wichtige Daten nicht nur lokal, sondern auch online zu sichern. Dazu stellt Novastor kostenlos Online-Speicher zur Verfügung. Zudem können auch andere Speicherorte oder beliebige FTP-Server verwendet werden. Auch neu ist die Disk-Image-Funktionalität, dank der sich Systeme rekonstruieren lassen.

### Business-Automation
Das auf Business Automation spezialisierte Unternehmen Opacc hat die Version 13 seiner Software-Suite Opacc One lanciert. Technologisch gesehen ist der Hauptkern in der aktuellen Ausgabe die Einführung eines Service-Bus. Er soll Benutzer und Anbieter von Diensten so miteinander verbinden, dass sich auch Drittanwendungen auf Consumer- oder Providerseite einbinden lassen.

### Lieferzentrum
Citrix hat drei neue Komponenten für sein Delivery Center vorgestellt. Citrix Desktop Receiver und Citrix App Receiver sind zwei Software-Clients, die auf den Geräten der Endanwender dafür sorgen sollen, dass zentralisierte Desktops und Applikationen mit optimaler Bedienfreundlichkeit bereitgestellt werden. Beide verfügen über eine erweiterbare Architektur, die Plug-ins unterstützt.

### Bewerbermanagement
Der deutsche Workflow-Automation-Spezialist IQ-Optimize hat seiner gleichnamigen Software eine neue Funktion zum Bewerbermanagement hinzugefügt. Damit soll dieser Prozess in einem strukturierten Workflow zusammengefasst und so deutlich Zeit gespart werden. Konkret sollen damit Blindbewerbungen nach Kriterien wie den Qualifikationen des Bewerbers direkt an die zuständige Stelle weitergeleitet werden können.

### Vom Mainframe zur SOA
Micro Focus lanciert eine neue Version von SOA Express, mit der sich Enterprise-Applikationen auf IBM-Mainframes in eine serviceorientierte Architektur überführen lassen. In der neuen Ausgabe wurde die Infrastruktur vereinfacht. Durch die Software generierte Web-Services sollen sich ohne Einschaltung eines Applikationsservers in das Transaktionssystem CICS einfügen lassen.

# Mobile Computing als Sicherheitsleck

Mobile Computing ist aus der heutigen Arbeitswelt kaum mehr wegzudenken. Damit einher gehen aber auch Gefahren. Dieser Artikel weist auf mögliche Stolpersteine für Unternehmen hin und zeigt, wie man sie beseitigen kann.

Mobile Computer werden immer vernetzter. Mittlerweile verfügen selbst die günstigsten Notebooks neben einem Ethernet-Anschluss auch über kabellose Kommunikation mittels Bluetooth, W-Lan und Infrarot. Dank kontinuierlich sinkenden Datenübermittlungskosten statten zudem immer mehr Unternehmen und Private ihre Notebooks mit Datenkarten aus und ersetzen die klassischen, nur für Telefonate oder SMS genutzten Handys, durch Smartphones. Doch die gewonnene Mobilität hat auch sicherheitsbezogene Nachteile.

Mitarbeiter mit Reisetätigkeiten benötigen sichere Mobilität zu niedrigen Kosten. Die verwendeten Laptops benötigen Internet-Zugang über öffentliche Access-Points, über Nutzung von privaten Breitbandanschlüssen sowie für den Intra- und Internetzugang und die Synchronisation mit Business-Smartphones. Ein Unternehmen muss auch für alle Arten von mobilen Geräten die Anforderungen der IT-Security sicherstellen.

Deshalb ist es schlichtweg fahrlässig, den möglichen Verlust oder Diebstahl eines Laptops nur mittels Kauf eines Ersatzgerätes abzusichern. Ein Unternehmen muss sicherstellen, dass heikle Informationen nicht ungewollt die Firma verlassen und ihr Ansehen, zum Beispiel durch den Verlust von sensiblen Kundendaten, nicht geschädigt werden kann. Es reicht daher auch nicht, mobile Geräte nur durch die Verschlüsselung der gespeicherten Daten abzusichern. Denn wenn ein Laptop in fremde Hände fällt, wird die Verschlüsselung der Daten für einen Dieb oder Hacker nur den erfolgreichen Zugriff auf sensitive Daten verzögern.

Insbesondere folgende Risiken müssen für das mobile Arbeiten innerhalb und ausserhalb der Unternehmung mitberücksichtigt werden:

- Diebstahl oder Verlust des Gerätes
- Fehlende Sicherheitsmechanismen des Unternehmensnetzwerks wie Firewall, Reverse Proxy, IDS, automatische Aktualisierung von Antivirenschutz und Sicherheitsupdates
- Erhöhte Bedrohung durch Malware, Trojaner und Viren sowie temporär deaktiviertem Antivirus- und Malwareschutz

Gute mobile Sicherheit und guter Datenschutz basieren darum auf der Einführung eines ganzheitlichen Verfahrens, das konzeptionelle und technische Sicherheitsaspekte beinhaltet.

### Konzept und Technik sind zentral
Eine obligatorische Security-Policy als rechtliche Grundlage muss die Leitplanken für alle Benutzer eines Unternehmens definieren. Deshalb müssen alle Mitarbeiter an Security-Awareness-Trainings teilnehmen, welche die Erklärung der Bedeutung von Informations-Sicherheit für die unternehmensweite Einhaltung von gesetzlichen Richtlinien beinhalten. Viele Tipps scheinen banal und selbstverständlich, aber trotzdem werden oft Mobile Devices unbeaufsichtigt an undenkbaren Orten liegen gelassen.

Wichtige Bestandteile eines Awareness-Trainings sind zudem eine Sensibilisierung mit dem Umgang mit Passwörtern und dem Clean-Desktop-Verfahren (Passwörter nicht aufschreiben, sensitive Kundendaten nicht einsehbar verwalten) und eine intensive Schulung gegen mögliche Social-Engineering-Attacken.

Basis der technischen Sicherheit für mobile Geräte sind unter anderem die Einführung starker Passwortregeln, zertifikatsbasierende Authentifikationsmechanismen, One-Time-Pads wie Secure ID, Hardware-Dongles und eine Clean-Desktop-Policy für alle Mitarbeiter. Weiter muss die Installierung und Aktivierung von Schutzmechanismen, wie passwortgeschütztem Bios-Bootlock, Verschlüsselung aller Laufwerke (bios-, partitions- oder drivebasiert) gewährleistet sein. Unerwünschte Dienste wie Infrarot, W-Lan oder Bluetooth sollten generell deaktiviert sein und bei Bedarf ausschliesslich über separate Hardware-Profile aktiviert werden können.

### Verschlüsselung ist zentral
Der Intranet-Zugang sollte zudem ausschliesslich über stark verschlüsselte VPN-Clients mit Security-Policy erfolgen. Bei bestehender VPN-Verbindung sollten alle anderen Verbindungen deaktiviert sein. Alle abgehenden Datenpakete dürfen nur durch den aufgebauten VPN-Tunnel gehen und nur Datenpakete aus dem Tunnel dürfen akzeptiert werden. Die Verbindung in das interne Netz sollte immer durch eine vorherige starke Authentisierung geschützt werden. Alle Authentisierungsinformationen, die für den Aufbau eines VPNs zwischengespeichert werden, sollten nach dem Ende der VPN-Nutzung automatisch gelöscht werden.

Schliesslich sollte der Internet-Zugang ausschliesslich per Routing über das Firmennetz zugelassen werden und die Nutzung aller Server-Dienste bedarf einer aktiven Protokollierung, um die erfolgten Zugriffe jederzeit nachvollziehen zu können.

Generell werden zudem periodisch durchgeführte technische Audits empfohlen, um die implementierte Sicherheit gegenüber der geltenden Security Policy zu überprüfen. Für viele Unternehmen in der Finanzbranche besteht sogar die Pflicht, ihre IT-Systemlandschaft und ihre Prozesse anhand solcher Tests mindestens jährlich überprüfen zu lassen, um internationalen Revisionsanforderungen wie dem Sarbanes-Oxley Act oder Basel II gerecht zu werden.

Zusammenfassend lässt sich sagen, dass Mobile Computing zum Alltag in jedem Unternehmen gehört. Die eingesetzten Geräte werden von den Mitarbeitern nahezu überall und jederzeit verwendet. Erst eine Implementierung einer ganzheitlichen, konzeptionellen und technischen Sicherheit deckt die für mobile Geräte notwendige Sicherheit und Vertraulichkeit ab, die in der Welt der tragbaren Geräte nicht mehr wegzudenken ist.

## DER AUTOR

René Hürlimann (35) ist Senior Consultant bei Oneconsult. Oneconsult ist ein international tätiges Schweizer IT-Security-Consulting-Unternehmen mit Schwerpunkt technische Audits. Oneconsult hat Büros in der Schweiz, Deutschland, Frankreich und Österreich.
www.oneconsult.com