

SECURITY UNTERWEGS

Schutz der mobilen Geräte



Das mobile Gerät ist zu einem ständigen Begleiter geworden. Sei es nun ein Handy, ein Smartphone oder ein Notebook, die wichtigsten Daten sind immer mit dabei. Oft sind hier sehr vertrauliche Informationen gespeichert, die in den falschen Händen einen grossen Schaden verursachen könnten. Umso wichtiger ist der Schutz dieser Geräte.

AUTOR: ANDREAS WISLER

Eine Statistik von Web & Collaboration Strategies geht davon aus, dass 10 Prozent aller Notebooks gestohlen werden, 70 Prozent dieser Diebstähle sogar in Gebäuden! 98 Prozent der Notebooks tauchen dabei nie mehr auf. Erschreckend ist auch eine Auswertung von London Tourismus, bei welcher zwischen Juli und Dezember 2004 63 000 Handys, 5 800 PDAs und 5 000 Notebooks liegen blieben.

Sei es nun aus Unachtsamkeit oder Fahrlässigkeit, der Schutz dieser Geräte ist enorm wichtig. Selbst eine Agenda in falschen Händen kann schon viel über eine Firma und deren Beziehungen aussagen. Der Wert der verlorenen Daten ist nur sehr schwer bezifferbar. Studien von Ultimaco gehen davon aus, dass sich der Wert bei etwa 40 000 Dollar pro Ereignis bewegt, bei Laptops sogar gegen 90 000 Dollar.

Schutz auf Reisen

Auf Reisen sollte das mobile Gerät unauffällig transportiert werden. Eine Notebooktasche weckt bereits das Interesse. Eine gute Möglichkeit sind Rucksäcke, welche ein spezielles Fach für das Notebook haben. Weiter gehört das sichere Verstauen des mobilen Gerätes dazu. Im Zug oder im Flugzeug sollte

das wichtige Gepäck nicht in den oberen Gepäckfächern verstaut, sondern im vorderen Sitz versorgt werden.

Passwortschutz der Daten

Die Daten können auf verschiedene Arten geschützt werden. Als einfachste Methode bietet sich der Schutz mit einem Passwort. Ein Schutz vor fremden Zugriffen mit einem Passwort ist aber nicht immer sicher. Hier kommt es ganz stark auf die Art an. Achten Sie darauf, dass immer ein anerkanntes Verfahren mit einer hohen Sicherheit benutzt wird. Bei jedem Algorithmus gilt: je länger ein Passwort ist, desto sicherer. Oder in anderen Worten, der beste Verschlüsselungsalgorithmus nützt nichts, wenn ein triviales Passwort verwendet wird.

Verzeichnisschutz mit EFS

Mit dem Einsatz von EFS (Encrypted File System) ist es möglich, einzelne Dateien, Verzeichnisse oder die ganze Festplatte so zu verschlüsseln, so dass nur Befugte die Daten lesen können. EFS ist seit Windows 2000 im Lieferumfang enthalten.

Um ein Verzeichnis zu schützen, klicken Sie mit der rechten Maustaste auf das entsprechende Verzeichnis und wählen Sie unter dem Register „Allgemein“ den Punkt „Erwei-

„Auf Reisen sollte das mobile Gerät unauffällig transportiert werden.“

„... je länger ein Passwort ist, desto sicherer.“

Eigenes Intra- oder Extranet in nur 5 Minuten!

Die perfekte Lösung für schnelles und effizientes Arbeiten in KMU!

Grundfeatures von SharePoint:

- Terminverwaltung
- MS Office Integration
- Unlimitierte Anzahl Benutzer
- Dokumentenverwaltung
- Listenverwaltung
- Inhaltsverwaltung
- Diskussionsplattformen
- Individuelle Gestaltung
- Über 40 verschiedene Vorlagen
- Bildergalerie
- Umfragen-Tool
- u.v.m.

Jetzt anmelden und einen Monat lang gratis testen:
www.sharepointhosting.ch

SharePoint bei Genotec heisst:

- Zugriff auf alle Daten, Dokumente und Informationen
- Von überall erreichbar
- Teamsites, Projekte und Dokumentarbeitsbereiche wie Umfragen, Links und Tabellen sind sekundenschnell erstellt
- Eigene Server-Infrastruktur entfällt
- Für sichere Daten, Virenschutz, Backup und Verfügbarkeit sorgt Genotec
- Alle nötigen Tools sowie Speicherplatz inklusive

 **genotec**



Microsoft
CERTIFIED
Partner

Genotec - Internetdienste ohne Kompromisse.

Mehr Informationen: Tel. 0848 321 123
www.genotec.ch
www.sharepointhosting.ch

tert“ aus. Hier setzen Sie ein Häkchen bei „Inhalt verschlüsseln, um Daten zu schützen“. Automatisch wird ein Zertifikat auf den Namen des eingeloggtten Benutzers ausgestellt. Nur mit diesem ist es möglich, zu einem späteren Zeitpunkt wieder auf die Daten zuzugreifen. Ein Backup davon lohnt sich daher auf jeden Fall. Dass die Verschlüsselung aktiv ist, zeigt Windows an der grünen Schrift an.

Dass EFS leider keinen absoluten Schutz bietet, zeigt das Tool „Advanced EFS Data Recovery“ (AEFSDR) der russischen Software-Firma ElcomSoft. Die Software, mit der schon unter Windows 2000 EFS-geschützte Dateien entschlüsselt werden konnten, funktioniert in der neuen Ausgabe auch unter Windows XP und Windows Server 2003.

Harddiskverschlüsselung

Als bisher unknackbar gelten Programme, welche die gesamte Harddisk verschlüsseln. Somit ist es auch nicht möglich, mit einer Unix-Boot-Disk auf die Daten zuzugreifen. An dieser Stelle seien nur zwei Programme erwähnt: SecureDoc und SECUDE secure notebook. Sollte auf Reisen einmal das Passwort vergessen werden, kann es bei beiden Programmen via den Administrator unterwegs „zurück“ gesetzt werden. Die oben genannten Möglichkeiten gelten dabei nicht nur für Notebooks, sondern auch für PDAs und Smartphones. Viele Hersteller haben die Gefahr erkannt und offerieren kostenlos ein entsprechendes Sicherheitsprogramm. Nun ist es nur noch wichtig, dass Sie dieses auch einsetzen und Ihre Daten vor fremden Zugriffen schützen. ◆

ZUM AUTOR

Andreas Wisler (Tel. 052 320 91 20), Dipl. Ing. FH, CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Portfolio ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) herunter geladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.



Wir lotsen Ihre Daten sicher ans Ziel!

Die **Kaspersky Hosted Security Services** schützen Unternehmens-Netzwerke jeder Größe zuverlässig vor Bedrohungen – inklusive Kontrolle der Internet-Nutzung.

Verlagern Sie die Administration Ihrer E-Mail- und Web-sicherheit an das Expertenteam der **Kaspersky Hosted Security Services**. So steigern Sie die Produktivität Ihrer Mitarbeiter und senken den Administrations-Aufwand sowie die Kosten für Hardware. Zudem profitieren Sie von automatischen Updates und dem Einsatz modernster Technologien. **Ihre Vorteile:**

- **Bester Schutz**
durch Einsatz neuester Sicherheits-Technologien
- **Verringerung des eingehenden Traffics**
durch Filter- und Quarantäne-Regeln
- **Höhere Mitarbeiter-Produktivität**
sowie Zeitersparnis, da das Aussortieren von Spam und Schadprogrammen entfällt
- **Flexible Skalierbarkeit**
durch problemlose Integration neuer Mitarbeiter und Niederlassungen mit minimalem Zeitaufwand
- **Optimale Ressourcen-Nutzung**
durch Auslagerung der Wartung und Pflege an die Kaspersky-Sicherheitsexperten
- **Garantierte Leistungsfähigkeit**
und Verfügbarkeit der Dienste (Service Level Agreements)

Wie auch Ihr Unternehmen optimal von den Kaspersky Hosted Security Services profitieren kann, erfahren Sie durch eine kostenlose Evaluierung unseres Services unter www.hostedsecurity.de

KASPERSKY Lab
www.kaspersky.ch