Die individuell beste Datenverschlüsselung

Maßgeschneiderter Zugriffsschutz

Spätestens wenn man ein Notebook oder einen USB-Stick mit sensiblen Daten verloren hat, wünscht man sich, die Daten wären verschlüsselt gewesen. Da es „die Verschlüsselungslösung“ nicht gibt, zeigen wir Ihnen verschiedene Lösungsansätze zur Verschlüsselung von Daten auf Datenträgern. So finden auch Sie die optimale Lösung für Ihr Unternehmen.

Auf der Festplatte eines Arbeitsplatzrechners oder auch eines Notebooks sind in Form von Textverarbeitungsdateien, Tabellenkalkulationsdateien, Datenbanken, E-Mails und vielen anderen Dateien personenbezogene und andere vertrauliche Daten gespeichert.

Nur die Festplattenverschlüsselung ist wirklich sicher

Der Dieb eines solchen Rechners kann Schutzmaßnahmen wie Bootschutz umgehen, indem er einfach die Festplatte des Rechners ausbaut, diese dann in einen anderen Rechner einbaut und dort ausliest. Deshalb ist nur die Verschlüsselung der Daten auf der Festplatte sicher.

Die Verschlüsselung einzelner Dateien ist die einfachste, aber nicht die sicherste Lösung

Die einfachste Art der Verschlüsselung ist das Verschlüsseln einzelner Dateien. Dies lässt sich mit vielen verschiedenen Programmen realisieren.

Ein solides Programm ist die Freeware Axcrypt. Utimaco Private Crypto ist in der Bedienung ähnlich einem Pack-Programm, hat aber seinen Schwerpunkt in der Verschlüsselung.

Auch Pack-Programme können verschlüsseln, erfordern aber das Engagement der Mitarbeiter

Prinzipiell kann auch jedes Pack-Programm zur Verschlüsselung genutzt werden. Leider hat gerade das populäre ZIP-Format mit seiner Standard-Verschlüsselung erhebliche Schwächen. Eine plattformübergreifende Empfehlung wären die Formate RAR (kommerziell) und 7z (GPL – General Public License – also freie Software).

Auswahl Verschlüsselungs-Tools

- **Verschlüsselung einzelner Dateien**
  - AXcrypt (Windows, GPL)
  - Utimaco PrivateCrypto (Windows, kommerziell)
  - GnuPG (Windows, Linux, Mac OS, GPL)
  - Pack-Programme (alle Betriebssysteme, verschiedene Lizenzen)
- **Containerverschlüsselung**
  - PGP Virtual Disk (Windows, Mac OS, kommerziell)
  - Utimaco PrivateDisk (Windows, kommerziell)
- **Container- oder Partitionsverschlüsselung**
  - TrueCrypt (Windows, Linux, TCL)
  - Loop-AES (Linux, GPL), kompatibel zu CrossCrypt (Windows, GPL)
- **Dateiverschlüsselung**
  - Utimaco LanCrypt (Windows, kommerziell)
  - Microsoft EFS (Windows, im Betriebssystem)
  - PGP NetShare (Windows, kommerziell)
- **Festplattenverschlüsselung**
  - Safeguard Easy (Windows, kommerziell)
  - PGP WholeDisk (Windows, Mac OS, kommerziell)
  - Bitlocker (Windows Vista, teilweise im Betriebssystem)

Beide unterstützen die starke AES-Verschlüsselung.

Bei dieser Art der Verschlüsselung ist das Unternehmen auf die aktive Mitarbeit der Beschäftigten bei der Verschlüsselung angewiesen. Automatisch geht hier (fast) gar nichts. Jede Datei muss manuell einzeln ver- und entschlüsselt werden.

Die Containerverschlüsselung bietet Komfort mit Macken

Bekannt und weit verbreitet sind sogenannte Containerverschlüsselungen. Bei diesem Verschlüsselungstyp wird eine große Datei erzeugt, die über die Software als Laufwerk verbunden werden kann. Alles, was Sie auf diesem Laufwerk speichern, wird dann automatisch verschlüsselt.

Conatiner-Dateien dürfen in der Regel auch auf Netzwerklaufwerken gespeichert werden. Aber der erste Nutzer, der den Container auf dem Fileserver öffnet, sperrt den schreibenden Zugriff für alle anderen. Bekannte Vertreter dieser Gattung sind PGPdisk, Utimaco Private Disk oder TrueCrypt.

Die Containervariante verschlüsselt nicht den Arbeitsspeicherinhalt

Mit dieser Art der Dateiverschlüsselung lässt sich allerdings die Windows-Auslagerungsdatei nicht verschlüsseln. Auch die Datei, die Windows im Ruhezustand nutzt, um den Arbeitsspeicherinhalt zu speichern, wird nicht verschlüsselt.

Die Produkte unterstützen teilweise die Schlüsselspeicherung auf Chipkarten, USB-Dongles oder TPM-Chips (Chipkarte auf dem Motherboard).

Die Partitionsverschlüsselung schützt vor ungewolltem Löschen

Einige Programme wie TrueCrypt kennen zusätzlich einen Modus zur Verschlüsselung einer Partition. Dies ist z.B. auf Notebooks praktisch.

Das Betriebssystem und die Programme liegen auf Laufwerk C. Das Laufwerk D – eigentlich die zugrunde liegende Partition – mit den Daten wird verschlüsselt.

Während eine Containerdatei versehentlich gelöscht werden kann, ist eine Partition davor geschützt. Aber auch hier werden die Auslagerungsdatei und die Ruhezustandsdatei ungeschützt, d.h. im Klartext, gespeichert.

Die Festplattenverschlüsselung bietet einen umfassenden Schutz

Bewährt haben sich Produkte wie z.B. Utimaco Safeguard Easy, die die komplette Festplatte oder Partition verschlüsseln und dadurch in der Lage sind, einen sicheren Bootschutz zu gewährleisten.

Ohne Eingabe des richtigen Passworts wird die Festplatte nicht entschlüsselt, und das Notebook bootet nicht.

Nur derartige Programme verschlüsseln sowohl die Auslagerungsdatei als auch die Ruhezustandsdatei.

Bei Windows Vista (Enterprise und Ultimate) hat Microsoft mit Bitlocker auch eine Festplattenverschlüsselung eingebaut. Sie stellt jedoch spezielle Anforderungen an die Hardware. Der Schlüssel muss in einem TPM-Chip der Version 1.2 gespeichert werden.

Alle diese Verschlüsselungsarten sind aber für ein Netzwerk ungeeignet

In Netzwerkumgebungen mit Teamarbeit nutzen die bisher diskutierten Lösungsansätze leider recht wenig:

- Die Containerverschlüsselung ist zwar in der Regel netzwerkfähig, aber nicht teamfähig, da der erste Nutzer, der den Container auf dem Fileserver öffnet, den schreibenden Zugriff für alle anderen sperrt.
- Und die Festplatten- bzw. Partitionsverschlüsselungen sind funktionsbedingt nicht netzwerkfähig.

Einzel-, Container-, Partitions-, Datei- oder Festplattenverschlüsselung? Für jedes „Fach“ gibt es passende Verschlüsselungs-Tools.

Für ein Netzwerk bieten sich Individuelle Dateiverschlüsselungen an

Bessere Lösungen stellen da individuelle Dateiverschlüsselungen dar, wie sie Utimaco Safeware mit LANcrypt oder PGP mit Netshare anbietet. Hier wird jeder Dateizugriff – ähnlich wie von einem On-Access-Virenscanner – abgefangen und geprüft, ob die Datei ver- oder entschlüsselt werden muss.

Die Verschlüsselungsregeln werden in der Konfiguration festgelegt und können z.B. alle Dateien in einem Verzeichnis, auf einem Laufwerk oder alle Dateien eines bestimmten Typs umfassen. Es spielt keine Rolle, ob die Datei auf einem lokalen oder einem Netzwerklaufwerk abgelegt ist.

Achten Sie auf Kompatibilität zwischen der Verschlüsselungssoftware und dem Virenscanner

Da diese Art der Verschlüsselung im Zugriffsmuster und in der Verankerung im Betriebssystem einem Virenscanner gleicht, können sich die Verschlüsselungssoftware und der Virenscanner auch in die Quere kommen. Hier sind unbedingt intensive Tests vor dem Einsatz erforderlich.

Zusammenfassung: Was wann wo wofür am besten einsetzen?

- Die Verschlüsselung einzelner Dateien ist dann geraten, wenn eine vertrauliche Datei als E-Mail-Anhang oder auf einem Datenträger verschickt werden soll.
- Container-Verschlüsselung lässt sich sinnvoll auf USB-Sticks einsetzen.
- Auf einem Notebook sollte zumindest die Datenpartition verschlüsselt werden, besser ist eine komplette Verschlüsselung der Festplatte.
- Bei Notebooks sind Enterprise-Funktionalitäten wie Challenge-Response oder Einmalpasswörter unerlässlich. Nur so kann man einem Mitarbeiter unterwegs helfen, wenn er sein Passwort vergessen hat.
- Gruppenstrukturen im Unternehmen mit entsprechenden Zugriffsrechten setzen eine entsprechende Dateiverschlüsselung voraus.

Sorgfältige Planung vor Einführung einer Verschlüsselung ist ein Muss

Jede Verschlüsselung verlangt eine sorgfältige Planung vor der Einführung. Sonst sind irgendwann die Schlüssel und Passwörter weg und damit auch die vertraulichen Daten. Und das will sicher niemand.

Prof. Dr. Rainer W. Gerling

Kostenlose Artikel-Downloads für Abonnenten

Lesen Sie auch die Artikel über die Verschlüsselungs-Tools

- Axcrypt – Elektronische Post unter 4 Augen *http://www.interest.de/DP/ausgaben.php?art=385*
- TrueCrypt – Mit verschlüsselten Laufwerken sicher unterwegs *http://www.interest.de/DP/ausgaben.php?b=new&art=341*