2 Sicherheit

Immer neue Malware gefährdet Daten und nutzt teilweise seit Längerem bekannte Sicherheitslücken, um sich auszubreiten. Die jüngste Generation von Schad-Software ist überaus heimtückisch und hat ein riesiges Schadenspotenzial. Für einen sicheren PC brauchen Sie die richtigen Tools. Sie dienen der Schädlingsprävention und dem Schutz vertraulicher Daten.

2.1 Die besten Security-Tools

Surfen im Internet funktioniert mit den serienmäßigen Browsern von Windows und Linux problemlos. Allerdings sorgen erst schlaue Tools für mehr Komfort, Sicherheit und Features. Beispielsweise lassen sich mit dem entsprechenden Tool die Passwörter für die mittlerweile oft unzähligen Logins viel besser verwalten als durch das simple Speichern der Daten im Browser.

Wie schützen Sie eigentlich Ihre Daten auf dem Computer vor ungewolltem fremden Zugriff? Soll beispielsweise nicht jeder, der an Ihrem Rechner arbeitet, Zugriff auf Ihre vertraulichen Daten haben – kein Problem, Tools schaffen hier und bei anderen sicherheitsrelevanten Gebieten Abhilfe.

Im Folgenden haben wir eine Auswahl an Tools und Utilities zusammengestellt, die die tägliche Arbeit an vielen Stellen deutlich sicherer machen und erleichtern.

2.1.1 ArchiCrypt USB-Protect – Laufwerke und Verzeichnisse verschlüsseln

Sicherheitsrelevante Daten müssen auf Computern oder Speichermedien wirkungsvoll vor fremden Zugriffen geschützt werden. ArchiCrypt USB-Protect (www.archicrypt.de) ver- und entschlüsselt Laufwerke und Verzeichnisse und kann sie als virtuelle Laufwerke dem Anwender sicher zur Verfügung stellen.

Funktionalität: Die Software ArchiCrypt USB-Protect erstellt verschlüsselte Laufwerke und Verzeichnisse, die auch als virtuelle Laufwerke angezeigt werden können. Geschützt werden die Daten innerhalb des verschlüsselten Laufwerkes mit einem sicheren Passwort. ArchiCrypt USB-Protect eignet sich zudem zur Verschlüsselung von Wechseldatenträgern wie USB-Sticks oder Flash-Speicherarten. Dabei wird das Verschlüsselungsprogramm als ausführbare Datei in das Verzeichnis beziehungsweise Laufwerk kopiert.

Auf Basis einer verschlüsselten „Datei“ erzeugt das Programm virtuelle Laufwerke. Bei der Verschlüsselung stehen die Schutzstufen Basisschutz (keine Verschlüsselung, sehr schnell), Mittlerer Schutz (Teilverschlüsselung, schnell) und Höchster Schutz (Vollverschlüsselung, schnell) zur Verfügung.

Installation: Die Installation unter Windows ist sehr einfach: die Setup-Datei herunterladen, starten, den Anweisungen folgen – fertig. Für Wechselmedien wie etwa einen USB-Sticks muss der Anwender entweder die mobile Version von ArchiCrypt USB-Protect auf den Stick kopieren oder die USB-Vorbereitung über das auf einem Rechner installierte Programm selber vornehmen. Schließt man das Wechselmedium an einen anderen PC an, wird von dort per autorun.inf automatisch die portable Version gestartet.

ArchiCrypt USB-Protect: Mit dem Tool lassen sich alle Arten von Laufwerken und Verzeichnisse komfortabel ver- und entschlüsseln.

Bedienung: Das Programm ist logisch gegliedert. Das Anlegen von verschlüsselten Laufwerken oder Verzeichnissen erfolgt problemlos durch eine intuitive Programmführung. ArchiCrypt USB-Protect bietet in jedem Fenster eine ausführliche Hilfefunktion an, die das Lesen des Handbuchs überflüssig macht.

Zugang zu einem Laufwerk oder Verzeichnis erhalten Sie ausschließlich nach Eingabe des von Ihnen festgelegten Passworts. Beim Speichern verschlüsselt ArchiCrypt USB-Protect Ihre Daten automatisch, die Entschlüsselung erfolgt unmittelbar beim Öffnen der Datei.

Fazit: ArchiCrypt USB-Protect ist eine einfach zu bedienendes Verschlüsselungsprogramm für Laufwerke oder Verzeichnisse. Es ist sowohl auf einem Windows-PC als auch auf einem portablen Medium wie einem USB-Stick nutzbar. Der Anwender kann das kostenpflichtige Tool als mobile Variante, ohne Installation und sogar ohne besondere Rechte an jedem Windows-Rechner nutzen.

- **Version:** 2.0.3
- **Hersteller:** Patric Remus
- **Download:** www.archicrypt.com/downloads.html
- **Sprache:** Deutsch
- **Preis:** Testversion mit eingeschränkter Funktionalität; Vollversion: 24,95 Euro
- **System:** Windows 8, 7, Vista, XP, Windows Server 2000 / 2003
- **Alternativen:** TrueCrypt, AxCrypt, CrossCrypt, DiskCryptor, dm-crypt, FreeOTFE, PGP Whole Disk Encryption, Steganos Safe 2008

2.1.2 BoxCryptor – Dateien für die Cloud verschlüsseln

Immer mehr Benutzer vertrauen ihre Daten den Anbietern von Cloud-Diensten an. Das ist komfortabel, aber nicht unbedingt sicher, wie Einbrüche bei Dropbox gezeigt haben. Die Software BoxCryptor (www.boxcryptor.com) bietet besseren und wirksamen Schutz dank starker Verschlüsselung.

Funktionalität: Mit BoxCryptor lassen sich Daten nach dem AES-256-Standard, einem Algorithmus mit einem sehr hohen Maß an Sicherheit, verschlüsseln. Dazu erstellt das Tool einen Ordner, in dem die codierten und mit einem Passwort geschützten Daten landen. BoxCryptor erkennt eine bestehende Dropbox-Installation und schlägt vor, den eigenen Ordner dort als Unterverzeichnis anzulegen.

Zusätzlich erstellt das Programm ein virtuelles Laufwerk und bindet es mit einem vom Benutzer wählbaren Laufwerksbuchstaben in Windows ein. Legt man dort Dateien ab, verschlüsselt das Tool sie automatisch und speichert sie im zugrunde liegenden BoxCryptor-Ordner. Über das virtuelle Laufwerk hat der Anwender Zugriff auf die unverschlüsselten Dateien, die beim Lesen in Echtzeit decodiert werden. Die kostenlose Version schützt maximal ein Drive vor neugierigen Blicken und verschlüsselt keine Dateinamen.

BoxCryptor steht für Windows, Linux, Mac OS X, iOS und als App für Android zur Verfügung. Allerdings kann man einen mit BoxCryptor in Windows verschlüsselten Ordner dank der Kompatibilität mit dem Encryption File System (EncFS) unter Linux und Mac OS X nutzen. Die genaue Vorgehensweise erläutert der Hersteller in seinem Blog (http://blog.boxcryptor.com).

Sicher ist sicher: Das Verschlüsselungsverzeichnis von BoxCryptor wird über ein virtuelles Laufwerk in Windows eingebunden.

Installation: Die Installation erfolgt unter Microsofts Betriebssystem Windows-typisch per Assistent, der nach Aufrufen der Setup-Datei startet.

Bedienung: Nach der Installation verhält sich das Tool weitgehend transparent. Alles, was der Anwender im virtuellen Laufwerk speichert, landet zuverlässig und verschlüsselt im BoxCryptor-Ordner. Lediglich ein Icon im Info-Bereich der Taskleiste verrät, dass die Software im Hintergrund aktiv ist. Ruft man per Rechtsklick

auf das Programmsymbol das Kontextmenü auf, lässt sich zum Beispiel der Laufwerksbuchstabe für das virtuelle Laufwerk oder das Passwort ändern.

In den kommerziellen Versionen verschlüsselt das Tool nicht nur den Inhalt von Dateien, sondern auch deren Namen. Dieses Verhalten lässt sich beim Anlegen eines BoxCryptor-Ordners anpassen. Auch können Daten bei mehreren Providern verschlüsselt werden. Die kostenlose Version ist auf einen Dienstleister beschränkt.

Fazit: BoxCryptor ist ein einfach zu bedienendes Programm, mit dem selbst Einsteiger keine Schwierigkeiten haben dürften, ihre Daten sicher zu verschlüsseln. Auf diese Weise lassen sich Cloud-Angebote wie Dropbox mit deutlich weniger Bedenken nutzen. Wer eine andere Plattform als Windows einsetzt, kann verschlüsselte Ordner dank EncFS zumindest unter Linux und Mac OS X verwenden.

- **Version:** 2.0.401.172
- **Hersteller:** Acombar
- **Download:** www.boxcryptor.com/download/
- **Sprache:** Deutsch und andere
- **Preis:** kostenlose Free-Version mit Basisfunktionen;
  Unlimited Personal: 36 Euro/Jahr, Unlimited Business: 72 Euro/Jahr
- **System:** Windows, Mac OS X, Linux, iOS, Android
- **Alternativen:** SecretSync, TrueCrypt

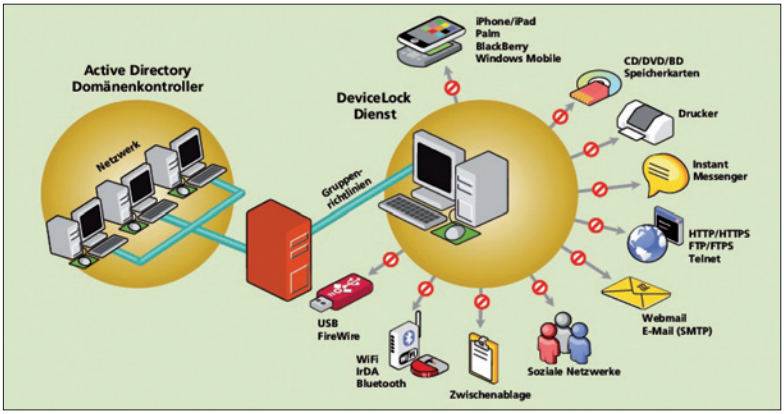
2.1.3 DeviceLock – USB und Firewire sperren

USB-Sticks und andere Wechseldatenträger zählen zu den elementaren Sicherheitsbedrohungen in Unternehmen. Mit dem Sicherheits-Tool DeviceLock (www.devicelock.com/de/) können Administratoren steuern, welche Benutzer Zugriff auf Schnittstellen wie USB, Bluetooth oder Firewire haben.

Funktionalität: Dass USB-Geräte für Unternehmen ein hohes Sicherheitsrisiko darstellen, belegen zahlreiche Studien. Auf diesem Weg gelangt einerseits Malware ins Unternehmen, andererseits können so kritische Daten das Unternehmen ganz einfach verlassen. Mit dem kommerziellen Sicherheits-Tool DeviceLock kann der Administrator die Verwendung der Schnittstellen kontrollieren. So kann die Nutzung von bestimmten Geräten unterbunden werden. Es lässt sich steuern, welche Anwender oder Gruppen Zugriff auf USB, WLAN, Bluetooth oder Firewire haben. Über eine USB-Whitelist kann man nur bestimmte USB-Geräte zulassen.

Per Medien-Whitelist kann der Administrator festlegen, dass der Anwender nur auf ganz bestimmte CD- oder DVD-Medien in seinem Laufwerk zugreifen darf. Einzelne Geräte lassen sich als Read-Only definieren. Ebenso kann der Administrator steuern, auf welche Art von Dateitypen auf Wechseldatenträgern wie zugegriffen werden darf. Es lassen sich Berichte erstellen, welche Geräte auf welche Art und Weise auf den Clients genutzt werden. Von allen Daten, die auf externe Geräte oder mit Windows Mobile synchronisiert werden, lassen sich auf einem zentralen Server Shadow-Kopien anlegen. DeviceLock unterstützt auch Endgeräte mit iOS-,

Android- und Windows-Phone-Betriebssystemen. Die Zugriffe auf BlackBerrys, iPhones und iPod Touch können beschränkt werden, außerdem sind Auditing- und Shadowing-Funktionen integriert.



Schnittstellenkontrolle: Mit DeviceLock können Administratoren eine Vielzahl von Geräteklassen und den Zugriff darauf kontrollieren.

Installation: Der Download von DeviceLock ist rund 187 MByte groß. DeviceLock kann als 30-tägige Demo mit vollem Funktionsumfang genutzt werden. Eine Einzellizenz kostet 47,60 Euro, Mehrplatzlizenzen sind je nach Anzahl deutlich günstiger. DeviceLock läuft unter Windows 7/NT/2000/XP/Vista sowie Windows Server 2003/2008. Administratoren können DeviceLock remote auf den Anwender-Clients installieren. Um DeviceLock zu installieren, muss man über Administratorrechte verfügen.

Bedienung: Zu DeviceLock gehören drei Komponenten. Der *DeviceLock Service Settings Editor* ist der Agent auf dem Client-System läuft und den Laufwerkschutz bietet. Der *DeviceLock Enterprise Manager* erlaubt eine zentralisierte Sammlung und Speicherung der Shadow-Daten. Über die *DeviceLock Management Console* können Administratoren das Client-System mit dem DeviceLock-Service aus der Ferne verwalten. Per Settings-Editor kann man komfortabel menügesteuert die Beschränkungen für die einzelnen Schnittstellen einrichten. So lassen sich Zugriffe beispielsweise auf Read-only beschränken. Zudem sind bestimmte zeitliche Einschränkungen möglich, ebenso das Anlegen von Whitelists für USB-Geräte. Man kann den Dienst so konfigurieren, dass Anwender mit lokalen Administratorrechen diesen nicht deaktivieren können.

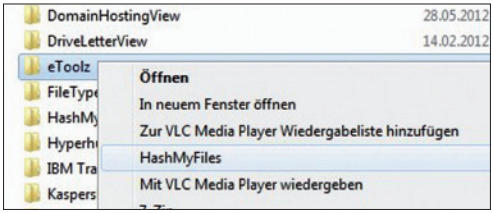
Fazit: Mit DeviceLock kann man eine Sicherheitsstrategie in Sachen Data Leak Prevention praktisch umsetzen. Die Software wurde ständig verbessert, vor allem die Verwaltungsfunktionen rund um Smartphones sind praktische und sinnvolle Erweiterungen.

- **Version:** 7.1.36106
- **Hersteller:** DeviceLock
- **Download:** www.devicelock.com/de/dl/download.html
- **Sprache:** Englisch, Deutsch
- **Preis:** Einzellizenz: 47,60 Euro, Mehrplatzlizenzen günstiger gestaffelt, 30-Tage-Demo-Version zum Download
- **System:** Windows NT, 2000, XP, Vista, 7, Windows Server 2000 / 2003 / 2008 (32 und 64 Bit)

2.1.4 HashMyFiles – Integrität von Dateien kontrollieren

Windows bietet keine Bordmittel, um die Integrität von Daten anhand ihrer Hash-Werte zu prüfen. Die Freeware HashMyFiles (www.nirsoft.net) füllt diese Lücke. Das Gratis-Tool ist portabel nutzbar und besitzt eine deutschsprachige Oberfläche.

Funktionalität: Hash-Werte dienen dazu, Objekten einen eindeutigen, nur einmal vorkommenden Wert zuzuweisen. Mithilfe dieser Prüfsumme, die zum Beispiel ein Softwareanbieter bereitstellt, lässt sich daher leicht feststellen, ob Daten unversehrt sind oder verändert wurden. Auf diese Weise ist es möglich, sich etwa vor manipulierten Programmen zu schützen. HashMyFiles berechnet die Hash-Werte von einer oder mehreren Dateien. Das Tool unterstützt dabei neben den Algorithmen MD5 und CRC32 die SHA-Varianten SHA-1, SHA-256, SHA-384 und SHA-512. Die ermittelten Werte lassen sich einfach in die Zwischenablage übernehmen und im Text-, HTML-, XML- oder CSV-Format speichern.



Direkter Aufruf: Das Tool lässt sich auch im Windows-Explorer über das Kontextmenü von Dateien und Ordnern nutzen.

Installation: HashMyFiles ist als portable Anwendung konzipiert. Daher reicht es aus, das Zip-Paket in ein beliebiges Verzeichnis zu entpacken und *HashMyfiles.exe* zu starten. Um das Tool mit der deutschsprachigen Oberfläche zu nutzen, muss man die passende Sprachdatei von der Herstellerseite herunterladen und die INI-Datei in denselben Ordner wie das Programm entpacken.

Bedienung: Der Anwender hat verschiedene Möglichkeiten, die Hash-Werte von Daten anzuzeigen. Am bequemsten gelingt dies, indem man Dateien und Ordner per Drag & Drop vom Windows-Explorer in das Programmfenster des Tools zieht oder das jeweilige Kontextmenü bemüht. Für die letztgenannte Methode muss man jedoch zunächst im Menü *Optionen* die Funktion *Im Explorer-Kontextmenü*

aufführen einschalten. Alternativ stehen die entsprechenden Befehle gleichfalls im Dateimenü parat. An dieser Stelle wird auch fündig, wer alle Files überprüfen möchte, die zu einem bestimmten laufenden Prozess gehören.

Das Tool präsentiert die mit einer der Methoden hinzugefügten Dateien in übersichtlicher Tabellenform. Anzahl und Reihenfolge der dargestellten Spalten lassen sich ebenso den persönlichen Vorlieben anpassen wie die Sortierung, die man mit einem Klick auf den jeweiligen Tabellenkopf umschaltet. HashMyFiles lässt sich auch über die Kommandozeile steuern. Die dazu erforderlichen Parameter findet man in der Readme-Datei und auf der Produktseite des Herstellers im Abschnitt *Command-Line Options* (www.nirsoft.net/utils/hash_my_files.html).

Fazit: Mit HashMyFiles findet der Anwender ein portabel nutzbares Tool, das die Hash-Werte von Dateien zuverlässig berechnet. Die deutschsprachige Oberfläche ist übersichtlich gestaltet, sodass sich auch Einsteiger sofort zurechtfinden.

- **Version:** 2.00
- **Hersteller:** Nirsoft
- **Download:** www.nirsoft.net/utils/hash_my_files.html
- **Sprache:** Deutsch und andere
- **Preis:** kostenlos
- **System:** Windows 2000, XP, Vista, 7, 8, Windows Server 2003
- **Alternativen:** Freehash, WinMD5Free

2.1.5 Lauschangriff – Verzeichnisse und Laufwerke überwachen

Um Ordner oder Laufwerke auf Löschungen, Umbenennungen, Kopieren oder Zugriffe zu überwachen, eignet sich das kostenlose Tool Lauschangriff (www.softwareok.de/?Download). Verschiedene Filteroptionen helfen bei der Analyse der gesammelten Informationen. Zusätzlich lassen sich die Ergebnisse der Überwachung als Datei exportieren.

Funktionalität: Auf der eigenen Festplatte, auf Wechselmedien oder auf Netzlaufwerken geschieht oft mehr, als man gemeinhin annehmen möchte. Und die Akteure müssen dabei keineswegs immer Schadprogramme sein. Mit Lauschangriff kann man Ordner oder ganze Laufwerke überwachen und dokumentieren, was dort geschieht. Das Tool dokumentiert beispielsweise Schreibzugriffe sowie das Löschen. Kopieren und Umbenennen von Dateien. Ebenso werden Erstellzeitänderungen, Zugriffszeitänderungen, Dateiattribute und Sicherheitseinstellungen überwacht. Die ermittelten Daten lassen sich in die Formate xls, csv, txt oder html exportieren. Daten, die nicht überwachenswert erscheinen, wie etwa tmp-Dateien, kann man von der Überwachung ausnehmen. Mit der neuesten Version kann man Dateitypen per Filter zur Überwachung gezielt auswählen. Der Autor weist explizit darauf hin, dass das Programm zur Analyse und zu Lehrzwecken dient. Überwachung ohne Zustimmung ist nicht gestattet.