1.5 So schützen Sie Ihre Daten

Postkarten waren einmal ein probates Mittel, um Nachrichten zu versenden – dabei störte es in den damaligen Zeiten kaum jemand, dass wenigstens der Postbote den Inhalt dieses „Datenträgers" in Klarschrift mitlesen konnte. Was den Geheimhaltungsgrad angeht, so entsprechen die E-Mail-Nachrichten in der heutigen Zeit durchaus den früheren Postkarten. Hier kann jeder den Text einfach mitlesen, wenn er nur ein wenig Mühe und Sachverstand aufweist.

Was liegt also näher, als die Daten, die per E-Mail übertragen werden sollen, einfach zu verschlüsseln? Und wenn man gerade dabei ist, dann sollten doch bitte alle Daten auf der Festplatte und auf allen anderen Übertragungswegen ebenso wie bei Zugriffen über den Web-Browser, über eine VPN-Verbindung (Virtual Private Network) oder bei der Fernwartung nur noch verschlüsselt vorliegen.

Da die „universelle" Verschlüsselung, die mit einem Knopfdruck die gesamte IT sicher verschlüsselt, leider noch nicht existiert, haben wir in diesem Ratgeber einige beispielhafte Verschlüsselungsmethoden für die verschiedenen Einsatzzwecke und entsprechende Programme zusammengestellt.

1.5.1 Verschlüsselung einzelner Dateien

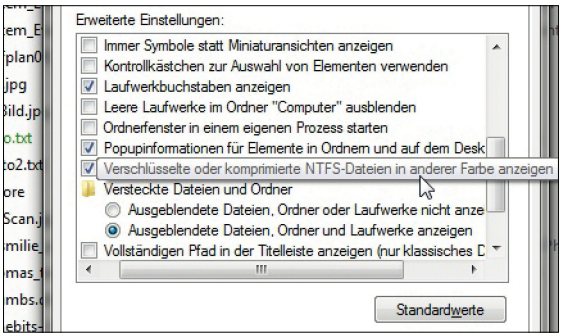
Wer ein halbwegs aktuelles Windows-System besitzt, der besitzt auch direkten Zugriff auf eine Verschlüsselung für Dateien und Ordner: Seit Windows 2000 steht für Datenträger, die mit NTFS (New Technology Filesystem – das Standard-Dateisystem der modernen Windows-Systeme) formatiert wurden, auch eine Dateiverschlüsselung zur Verfügung. Dieses Feature wird von Microsoft als EFS (Encrypting File System) bezeichnet. Die Bezeichnung ist allerdings etwas irreführend, da es sich nicht um ein Dateisystem handelt, sondern um ein Betriebssystem-Feature, das einzelne Dateien oder Ordner verschlüsseln kann.

Welche Vorteile bietet diese Verschlüsselungsmethode?

Sie ist einfach einzusetzen und direkt ins Betriebssystem integriert: ein Rechtsklick auf eine Datei oder einen Ordner, dann die Eigenschaften auswählen und dort bei den Attributen auf „Erweitert" klicken. Nach anschließender Auswahl von „Inhalt verschlüsseln, um Datei zu schützen" ist die Datei gesichert. Sie befindet sich nun verschlüsselt auf der Festplatte, während der Vorgang für den Anwender völlig transparent bleibt. Hat er bei den Ordneroptionen die entsprechende Einstellung gewählt, so wird er eine verschlüsselte Datei oder einen verschlüsselten Ordner nur an der anderen Farbe erkennen – beim Zugriff merkt er keinen Unterschied.

Aber wovor schützt diese Verschlüsselung? Sie schützt vor dem Zugriff eines anderen Anwenders, der ebenfalls auf diesem Rechner arbeitet oder vielleicht über das Netz auf ein solches Verzeichnis zugreift. Auch ein Administrator hat keinen Zugriff auf diese Dateien.

Verschlüsselte Dateien farblich kennzeichnen: Beim Dateizugriff bemerkt ein Anwender nicht, dass er auf eine verschlüsselte Datei zugreift. Hat er bei den Ordneroptionen die entsprechende Einstellung gewählt, so werden ihm diese Dateien aber in einer anderen Farbe angezeigt.

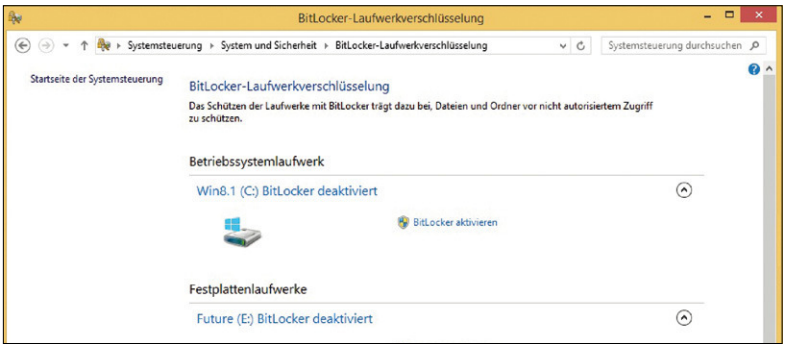


Welche Nachteile hat der Einsatz dieses Windows-Features?

Die Dateien sind immer noch sichtbar, die Methode funktioniert ausschließlich auf einem NTFS-Dateisystem und ist damit nur schlecht auf USB-Sticks oder Windows-Systemen einzusetzen, auf denen zumeist ein FAT-Dateisystem zum Einsatz kommt. Zudem ist es mit ihrer Hilfe nicht möglich, ganze Partitionen zu verschlüsseln.

1.5.2 Ganze Partitionen und Systeme verschlüsseln

Gerade was das Verschlüsseln von Partitionen angeht, hat Microsoft stetig weiter verbessert. So steht sowohl unter Windows 7 als auch unter Windows 8/8.1 mit Bitlocker nun eine Möglichkeit bereit, auch ganze Partitionen einschließlich der Systempartition zu verschlüsseln. Mit der seit Windows 7 vorhandenen „Bitlocker To Go"-Verschlüsselung können sogar ganze USB-Sticks und mobile Festplatten auf diese Weise verschlüsselt werden.



Gehört bei den professionellen Versionen von Windows 7 und Windows 8.x dazu: Bitlocker zur Verschlüsselung ganzer Partitionen.

Was können Anwender mit dieser Software verschlüsseln? Bitlocker verschlüsselt immer ganze Laufwerke beziehungsweise Festplattenpartitionen komplett. Auf diese Weise kann auch die Systempartition eines Windows-Systems vollständig verschlüsselt und damit gesichert werden. Ohne ein entsprechendes Passwort oder wahlweise eine Smartcard ist dann kein Zugriff auf dieses System mehr möglich. Ein besonderer Vorteil dieser Lösung: Auch sie arbeitet vollkommen transparent – hat der Anwender erst einmal sein Passwort eingegeben, so stellt sich ihm das System beziehungsweise die verschlüsselte Festplatte wie jedes andere Windows-System dar.

Welche Nachteile besitzt diese Technik?

Der größte Nachteile liegt wohl darin, dass Microsoft sie nur den „großen" Windows-Systemen spendiert hat: Nur die Windows-7-Versionen Ultimate und Enterprise sowie die Windows-8.x-Versionen Professional und Enterprise besitzen dieses Feature standardmäßig. Die anderen Windows-7- und Windows-8.x-Systeme können entsprechend vorschlüsselte Medien aber lesen, und auch für Windows XP stellt Microsoft eine entsprechende Anwendung für den lesenden Zugriff zur Verfügung.

1.5.3 Andere Verschlüsselungsmöglichkeiten

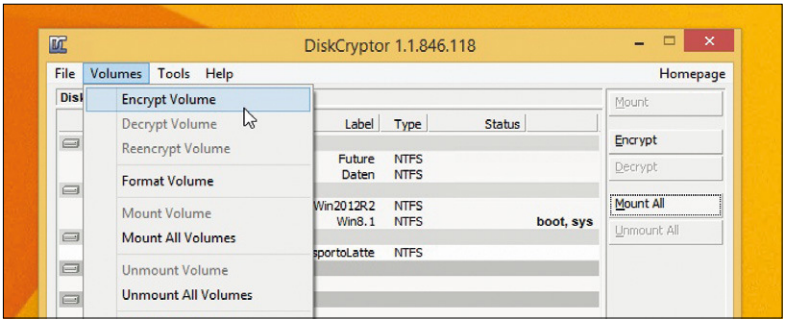
Was können Anwender tun, die keine entsprechende Windows-7-oder 8.x-Versionen im Einsatz haben? Bisher wurde ihnen von Experten immer wieder geraten, doch auf die bekannte Software **TrueCrypt** zurückzugreifen. Seit Mai 2014, als die Entwickler der freien Lösung plötzlich darauf hinwiesen, dass die Software nicht ausreichend sicher sei, und sie sofort die weitere Entwicklung der Software einstellten, ist dieser Tipp leider nicht mehr gültig.

Zwar ist noch nicht wirklich nachgewiesen, ob und welche Sicherheitslücken in TrueCrypt existieren, aber aufgrund dieser Unsicherheit raten die meisten Sicherheitsfachleute vom weiteren Einsatz der Software, deren Version 7.1 noch auf diversen Download-Portalen zu finden ist, dann doch ab. Eine ganze Reihe unterschiedlicher Softwarelösungen sowohl aus dem Freeware-Bereich als auch von kommerziellen Anbietern sind angetreten, die Nachfolge von TrueCrypt anzutreten. Leider reicht zum aktuellen Zeitpunkt in der zweiten Jahreshälfte 2014 noch keines dieser Programme an den Komfort und die Möglichkeiten von TrueCrypt heran.

Was bleibt nach TrueCrypt?

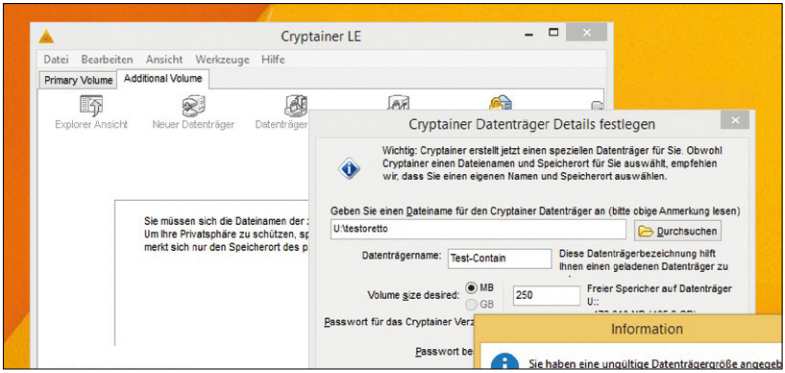
Wer auch weiterhin ganze Partitionen und dabei auch den Bereich der Festplatte, auf dem sich das Betriebssystem befindet, problemlos durch eine Verschlüsselung absichern will, dabei aber nicht auf Microsofts Bitlocker setzen möchte oder kann, der sollte einen Blick auf **DiskCrypter** (www.diskcryptor.net) werfen. Die Software ermöglicht es den Anwendern, ihre Systempartition mit den Verschlüsselungsalgorithmen AES, Serpent oder Twofish sichern. Es ist ebenso möglich, alle anderen Partitionen sowie Volumen auf externen Datenträgern wie USB-Festplatten oder -Sticks können zu verschlüsseln. Dabei ist das Programm offen und steht

komplett unter der GNU GPLv3-Lizenz zur Verfügung. Allerdings kann der DiskCryptor keine verschlüsselten Container-Dateien anlegen, wie es die Nutzer von TrueCrypt kennen und vielfach schätzen gelernt haben.



DiskCryptor macht es möglich: Ganze Partitionen mit einer Open-Source-Lösung sicher verschlüsseln.

Aber auch in diese Bresche springen bereits einige Programme. Dazu zählt unter anderem das Programm **Cryptainer LE** (www.cypherix.de/prods.htm), das von der Firma Cypherix in einer Freeware-Version angeboten wird. Es handelt sich dabei um eine „abgespeckte" 128-Bit Festplatten-Verschlüsselungssoftware Cryptainer PE und Cryptainer. Die Software erstellt in der gewohnten Weise Datei-Container, in die Nutzer dann per Maus sowohl Dateien und Verzeichnisse als auch E-Mail-Nachrichten hinziehen und dann verschlüsselt abspeichern können. Die größte Einschränkung dieses Programms besteht allerdings darin, dass es in der Freeware-Version nur eine Container-Größe von bis zu 100 MByte erlaubt. Allerdings können Nutzer problemlos mehrere dieser Container anlegen.



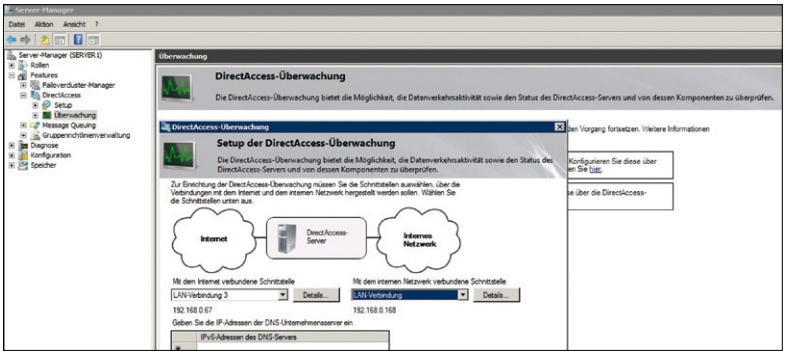
Cryptainer LE: Wenn es darum geht, verschlüsselte Datei-Container anzulegen, kann Cryptainer LE in der Freeware-Version eine mögliche Lösung sein.

Auch die österreichische Firma Braincell aus Graz stellt mit der Software **Protectorion PC Free** (http://de.protectorion.com/protectorion-togo/) eine für den Privatgebrauch freie Version ihrer Software bereit, die einfach einzusetzen ist und keine Größenbeschränkung für den Container besitzt, der hier als Daten-Safe bezeichnet wird. Die Freeware steht in zwei Versionen zum Download bereit: einmal als MSI-Datei für die Installation auf dem Desktop-Rechner und dann noch in der Version Protection ToGo Free, eine direkt ausführbare EXE-Datei für den Einsatz auf dem USB-Stick.

Als Verschlüsselungsalgorithmus kommt AES 256 (Advanced Encryption Standard) zum Einsatz, der nach wie vor als sicher gilt. Mit der freien Version der Software können Nutzer zwei Daten-Safes und eine Datei zum Abspeichern von Passwörtern für Webseiten anlegen und verwenden. Die Anzahl der darin verwalteten Daten ist laut Anbieter nicht begrenzt. Der Anbieter stellt auch einen Ausschnitt aus dem Source-Code seiner Software auf der Webseite zur Verfügung, um die Sicherheit seiner Lösung zu beweisen. Allerdings äußert es sich nicht weiter zu den Mechanismen und Verschlüsslungsvorgängen sowie deren Abläufe im Programm.

1.5.4 Lösungen fürs Firmennetz: VPN oder gleich Direct Access

Doch was tun die Profis, um beispielsweise eine sichere Verbindung zwischen den Netzwerken von Firmenstandorten zu gewährleisten? Hier sind VPNs (Virtual Private Network) die gängige Methode. Typischerweise werden sie als Appliance in der DMZ (Demilitarized Zone) verwendet und erlauben eine verschlüsselte und somit gesicherte Verknüpfung zwischen den Netzwerken. Allerdings besitzen beinahe alle diese Systeme eine Einschränkung: Nur wenn bei allen Verbindungen wirklich die Geräte eines Herstellers zum Einsatz kommen, ist sichere und verschlüsselte Übertragung wirklich gewährleistet.



DirectAccess von Microsoft: Zugriff auf das Unternehmensnetzwerk ohne zusätzliche VPN-Software.