



Virtual Private Drive

Rundum-Schutz für sensible Daten.

Wie sicher sind Ihre sensiblen Daten? Das Risiko von Missbrauch und Manipulation vertraulicher Informationen in Unternehmen hat sich durch die starke Verbreitung mobiler Arbeitsplätze, die ständige Verfügbarkeit von Daten und das einfache Abspeichern großer Datenmengen ständig erhöht.

Erst mit Hilfe von Datenverschlüsselung können diese Informationen auf PC, Notebook oder Wechselmedien zuverlässig geschützt werden - selbst bei Verlust oder Diebstahl der Hardware. Eine verschlüsselte Datei lässt sich nur von dem Benutzer entschlüsseln, der das entsprechende Passwort kennt oder im Besitz des benutzerspezifischen "Hardwareschlüssels" ist.

Keine Beeinträchtigung gewohnter Arbeitsabläufe

Einfache Administrierbarkeit

Virtual Private Drive ermöglicht dem Benutzer virtuelle, verschlüsselte Laufwerke sowohl lokal als auch in Netzwerken zu nutzen, die durch ein Passwort vor Fremdzugriff geschützt werden. Diese lassen sich nach der Verbindung wie gewöhnliche Windowslaufwerke verwenden.

Alle Daten wie Dokumente, Anwendungen oder Bilddaten werden sicher in einem Container gespeichert. Hierbei werden die kompletten Inhalte der Verzeichnisse und Unterverzeichnisse verschlüsselt. Die Ver- und Entschlüsselung läuft für den Benutzer transparent im Hintergrund und beeinträchtigt damit nicht die gewohnten Arbeitsabläufe.

Es kann mit bis zu 16 verschlüsselten Laufwerken gleichzeitig gearbeitet werden,

wobei jedes Laufwerk bis zu 1 TB (Terabyte) groß sein kann.

Zur Verschlüsselung nutzt Virtual Private Drive fortschrittliche und standardisierte Verschlüsselungsalgorithmen, die einen hochsicheren Schutz der vertraulichen Informationen gewährleisten.

Neben der manuellen Verbindung von Containerdateien über Passwordeingabe ermöglicht Virtual Private Drive auch eine automatische Verbindung, bei der die Passwörter verschlüsselt auf USB-Sticks, Smartcards oder anderen Hardware-schlüsseln abgespeichert werden. Damit kann der Benutzer nach seiner Authentifizierung sofort auf das verschlüsselte Laufwerk zugreifen und muss sich das Passwort nicht länger merken.

Virtual
Private
Drive

Virtual Private Drive

Betriebssysteme:

Microsoft Windows 2000/XP

unterschtützte Token:

- Alladin eToken
- Giesecke&Devrient Token
- GemSafe Xpresso
- Marx CrypToken
- SafeNet iKey
- Siemens SmartCard
- Wechseldatenträger

Standart:

PKCS#11

**Verschlüsselungs-
algorithmen:**

- AES
- Blowfish
- DES
- Dicrypt
- Triple-DES

Zentrale Administration

Über administrative Vorlagen für den Gruppenrichtlinieneditor kann zentral festgelegt werden, welche Virtual Private Drive Funktionen von wem und in welcher Weise genutzt werden können.

Durch die Vergabe von Berechtigungen besteht für den Administrator die Möglichkeit, die Erstellung von Containern durch Benutzer einzuschränken.

Eine Containerdatei lässt sich ohne zusätzlichen Aufwand in die vorhandenen Backupstrategien einbeziehen. Sie kann auch auf externe Speichermedien kopiert

oder per E-Mail versendet und an einer anderen Stelle wieder verwendet werden.

Starke Verschlüsselung

Zur Verschlüsselung werden die bekannten Verschlüsselungsalgorithmen AES, Blowfish oder Triple-DES verwendet. Zusätzlich steht Dicrypt, ein spezielles Verfahren von digitronic, zur Verfügung, welches beste Performance bietet.

Auf Datenträgern, die mit NTFS formatiert sind, werden die Container standardmäßig als "Sparsefiles" angelegt, so dass sie nur genau den Speicherplatz der tatsächlich enthaltenen Verzeichnisse benötigen und mit zusätzlichem Inhalt dynamisch wachsen.

Weitere Informationen finden Sie unter www.digitronic.net.

**digitronic
computersysteme gmbh**
Oberfrohaer Str. 62
D-09117 Chemnitz

Tel.: +49 (0) 371 815 39-0
Fax: +49 (0) 371 815 39-900
E-Mail: info@digitronic.net

