1 Deckblatt

Möglichkeiten der Datenübermittlung

der

DECODETRON Archiv-Service GmbH

Version	**01.01/0005**
Stand	**12.06.2009**
DocName	**DCT_Moeglichkeiten_der_Datenübermittlung_V0101.doc**

DECODETRON Archiv-Service GmbH · Siemensstrasse 17 · D-61449 Steinbach im Taunus
Telefon +49(0)700-77557766 · Telefax +49(0)700-77557766 · http://www.decodetron.de

2 Inhaltsverzeichnis

3 Allgemeines

3.1 Einleitung

Für die Übernahme Ihrer Daten, gleich welcher Art und Ursprung, stellt die deCODEtron Archiv-Service GmbH verschiedene Varianten zur Verfügung. Diese werden nach Übertragungsverfahren im folgenden Unterschieden.

3.2 Manuelle Datenübertragung

Bei der manuellen Datenübertragung kommen Hardware basierende Datenträger, wie Festplatten, CD/DVD, Tapes, usw. zum Einsatz. Diese Variante eignet sich besonders für sehr große Datenmengen und natürlich auch, wenn eine elektronische Übermittlung technisch nicht Möglich ist oder aus Sicherheitsgründen nicht in Frage kommt.

3.3 Elektronische Datenübertragung

Der Weg der elektronischen Datenübertragung bringt immer, je nach Wahl des Verfahrens mehr oder weniger, ein gewisses Risiko der Datenspionage mit sich. Um diesem Entgegen zu wirken haben wir verschiedene Verfahren zum Einsatz gebracht, die die elektronische Datenübertragung gegen Missbrauch sichern.
Zu diesem Zweck haben wir die verschiedenen Datenübertragungsmöglichkeiten, wie ISDN, Internet, Email usw. mit ganz unterschiedlichen Sicherungsmaßnahmen, wie .ZIP-Passwort, PGP/GnuPG/GnuPP-Verschlüsselung kombiniert und erhalten so auch ganz unterschiedlich sichere Verfahren.

4 Mögliche Datenträger mit manueller Handhabung

- Disketten
- ZIP-Disk
- CD-ROM
- DVD
- TAPE, Streamer, Bänder (siehe Tabelle unter Punkt 4)
- Festplatte SCSI, Type I, II, II
- Festplatte IDE ATA
- Festplatte IDE SATA
- Festplatte in Ext. Gehäuse mit Firewire IEEE 1394 oder USB 2.0
- MemoryCard kompatibel zu
- Compact Flash Card (CF) Type 1 und Type II
- IBM MicroDrive (MD)
- Smart Media Card (SM)
- SONY Memory Stick (MS)
- SONY Memory Stick Duo/Pro (MS, MSDuo, MSPro)
- XD Picture
- Secure Digital Card (SD)
- Multi Media Card (MMC) Type I, II
- RS Multi Media Card

5 Möglichkeiten der elektronischen Datenübertragung

- ISDN via AVM Fritz!-Data
- FTP via ISDN Direktverbindung
- Email
- FTP via Internet
- sFTP via Internet
- VPN-Tunnel via Internet

6 Datenformat, -Volumen, -Kompatibilität bei Datenträger mit manueller Handhabung

Datenträgerbezeichnung	Kompatibilität	Format	Max. Dateinamenlänge	Max. Volumen ca.
Disketten 3,5"	DOS, Windows	FAT	11 (8+3) Zeichen	1,44 MB
ZIP-Disk	DOS, Windows	FAT, FAT32	11 (8+3) Zeichen	100 MB
CD-ROM	DOS, Windows	DOS, ASCII, ISO 9660	11 (8+3) Zeichen, 31 Zeichen	650-700 MB
DVD ISO, UDF/ISO (+/-R; +/-RW)	DOS, Windows	DOS, ASCII, ISO 9660	11 (8+3) Zeichen, 31 Zeichen	4,4 GB (bis 2 GB/File)
DVD UDF (+/-R; +/-RW)	DOS, Windows	DOS, ASCII, ISO 9660	11 (8+3) Zeichen, 31 Zeichen	4,4 GB
TAPE Bandformat 3480 + 3490e	DOS, Windows	DOS, ASCII, Ebcdic, als TAR-File möglich. Feste Satzlänge (höchstens 255 Bytes), Blockgröße muss ein vielfaches der Satz-länge sein, aber höchstens 32.742 Bytes. Am besten ist ein Wert knapp über 10.000 Bytes.	11 (8+3) Zeichen	3490e = 2,5 GB
TAPE Streamer (QIC)	DOS, Windows	DOS, ASCII, Ebcdic. Blockgröße von 512 Bytes zwingend vorge-schrieben. Mögliche Formate: Tar, Snismc, As400 bis QIC525.	11 (8+3) Zeichen	bis 525 MB
TAPE Bandformat 8 mm	DOS, Windows	DOS, ASCII, Ebcdic. Bandlänge darf 112m oder 160m betragen. Mögliche Bandformate: Tar oder feste Satz-länge. Die Blockgröße im Tar-Format muss 512, 5120 oder 10240 Bytes betragen. Für feste Satzlänge gilt das gleiche wie unter Bandformat 3480 + 3490e beschrieben.	11 (8+3) Zeichen	bis 2,5 GB
TAPE Bandformat 4 mm DDS	DOS, Windows	DOS, ASCII, Ebcdic. DDS1 mit 60 m oder 90m, DDS2 mit 120 m und DDS3 mit 125 m Bandlänge. Mögliche Bandformate: Tar oder feste Satzlänge, an-sonsten gilt das gleiche wie bei 8mm	11 (8+3) Zeichen	DDS 1 60m=1,5 GB 90m=2,0 GB DDS 2 120m=4,0 GB DDS 3 125m=12,0 GB
Festplatte SCSI Typ I, II, III	DOS, Windows	FAT, FAT32, NTFS	11 (8+3) Zeichen, 31 Zeichen	Hersteller und Modell abhängig
Festplatte IDE ATA	DOS, Windows	FAT, FAT32, NTFS	11 (8+3) Zeichen, 31 Zeichen	Hersteller und Modell abhängig
Festplatte IDE SATA	DOS, Windows	FAT, FAT32, NTFS	11 (8+3) Zeichen, 31 Zeichen	Hersteller und Modell abhängig

Festplatte in Gehäuse mit Fire-wire IEEE 1394 od. USB 2.0	DOS, Windows	FAT, FAT32, NTFS	11 (8+3) Zei-chen, 31 Zeichen	Hersteller und Modell abhän-gig
Memor-yCard-Systeme Compact Flash Card (CF) Type I, II IBM MicroDrive (MD) Smart Me-dia Card (SM) SONY Me-mory Stick (MS) SONY Me-mory Stick Duo/Pro (MS, MSDuo, MSPro) XD Picture Secure Digital Card (SD) Multi Me-dia Card Type I, II (MMC) RS Multi Media Card (RSMMC)	DOS, Windows	Systemabhängig, Daten sollten DOS, ASCII, ISO 9660 konform sein	11 (8+3) Zei-chen, 31 Zeichen	System- und Hersteller abhängig

7 Übertragungsverfahren, Datenformat und Sicherheit bei elektronischer Datenübertragung

Übertra-gungsver-fahren	Daten-kompa-tibili-tät	Sicherheitsbewertung bei ungesicherten Daten *1	Zusätzliche Sicherungsmaß-nahmen (+ Be-wertung *1) / [+ Eignung*2]	Max. Datenvo-lumen ca.
ISDN via AVM Fritz!-Data	DOS, Windows	ausreichend (4)	- .ZIP-Passwort (2) [M+A] - PGP, GnuPG/GnuPP (1) [M+A]	Bis 50 MB/Tag, od. bis 100 MB nach Absprache
FTP via ISDN Direktver-bindung	DOS, Windows	befriedigend (3)	- .ZIP-Passwort (2) [M+A] - PGP, GnuPG/GnuPP (1) [M+A]	Bis 50 MB/Tag, od. bis 100 MB nach Absprache

Email	DOS, Windows	ungenügend (6), zusätzliche Sicherung unbedingt notwendig	- .ZIP-Passwort (5) [M] - PGP, GnuPG/GnuPP (1) [M] - Signatur empfohlen !	4-8 MB
FTP via Internet	DOS, Windows	mangelhaft (5), zusätzliche Sicherung sehr empfohlen	- .ZIP-Passwort (5) [M+A] - PGP, GnuPG/GnuPP (1) [M+A]	Bis 100 MB/Tag, od. bis 1000 MB nach Absprache
SFTP via Internet	DOS, Windows	gut (2)	Alle Verfügbaren, aber nicht notwendig	Bis 100 MB/Tag, od. bis 1000 MB nach Absprache
VPN Tunnel	DOS, Windows	sehr gut (1)	Alle Verfügbaren, aber nicht notwendig	Bis 100 MB/Tag, od. bis 1000 MB nach Absprache

*[1] Bewertung nach Schulnoten (1 = sehr gut, 2 = gut, 3 = befriedigend, 4 = ausreichend, 5 = mangelhaft, 6 = ungenügend)
*[2] A = **A**utomatische Datenverarbeitung (für z.B. Internetarchiv mit täglicher oder häufigere Datenaktualisierung), M = **M**anuelle Datenverarbeitung

8 Datensicherungsmaßnahmen

8.1 .ZIP-Passwort

Als Möglichkeiten der Datensicherungsmaßnahmen gegen unbefugten Zugriff stehen zum einen Passwortgeschützte .ZIP-Archive (auch bei automatischer Verarbeitung der Daten) zur Verfügung. Das mit uns abzustimmende ZIP-Passwort sollte in jedem Fall kryptisch sein, sprich aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Je länger das kryptische Passwort dann eingerichtet wird, desto sicherer sind die darin enthaltenen Daten. Selbst einschlägige Hacker-Sites bieten lediglich solche Knackprogramme an, die dem Passwort über einen "Brute Force-Attack" auf die Spur kommen. Das ist schlicht das Ausprobieren aller möglichen Kombinationen von Buchstaben, Zahlen und Sonderzeichen. Weitere Informationen zu sicheren Passworten finden Sie unter "Sichere Passworte". Bitte beachten sie aber, dass ZIP-Passworte keinen wirklich sicheren Schutz bieten, sondern lediglich solche Datenspione abhalten, deren Fachwissen nicht sonderlich groß ist.

8.2 Einfache Verschlüsselung

Ebenso können Verschlüsselungsverfahren zur Anwendung kommen, wie Sie Beispielsweise in PowerArchiver (www.powerarchiver.com) als Anwendung zur Verfügung stehen (Blowfish 128-bit; DES 56-bit; Tripple DES

168-bit; Rijndael - AES 128-bit, Rijndael - AES 256-bit). Die Anwendung eines dieser Verfahren muss allerdings zuvor mit uns abgestimmt und koordiniert werden. Im weiteren können natürlich auch andere Programme wie 7-ZIP, WinRAR, WinZIP, IZarc (um nur einige wenige zu nennen) verwendet werden.

8.3 Splitten und einfache Verschlüsselung

Auch möglich ist das Splitten und Verschlüsseln einer oder mehrer großer Dateien nach den folgenden Methoden: UUencode, XXencode, BASE64 (MIME), yENC. Die Anwendung eines dieser Verfahren muss allerdings zuvor mit uns abgestimmt und koordiniert werden.

8.4 PGP - Professionelle Verschlüsselung

Selbstverständlich bieten wir einen 4096-bit (bzw. 2048-bit bei automatischer Verarbeitung) starken Key zum Verschlüsseln mit PGP (www.pgp.com) an. Mit dieser Form der Datenverschlüsselung setzen wir die wohl stärkste Waffe gegen Neugierige ein. Unseren PublicKey erhalten Sie gerne auf Anfrage. Ebenso stehen wir Ihnen auch gerne mit Rat und Tat zur Seite. PGP selbst setzt eine lizenzierte Version für den gewerblichen Nutzer voraus. Alternativ kann auch GnuPG/GnuPP zur Anwendung kommen.

8.5 GnuPG/GnuPP - Professionelle Verschlüsselung

Als kostenlose und lizenzfreie Alternative zu PGP, für private ebenso wie für kommerzielle Anwendungen, stehen die Projekte GnuPG (www.gnupg.com) und GnuPP (www.gnupp.de) zur Verfügung. GnuPP findet dabei als Partner der Aktion "Sicherheit im Internet" (www.sicherheit-im-internet.de) des BMWA - Bundes-ministeriums für Wirtschaft und Arbeit (www.bmwa.bund.de) und des BMI - Bundesministeriums des Innern (www.bmi.bund.de) sogar Unterstützung von öffentlicher Seite. Beide Versionen werden von unserem PublicKey voll unterstützt. Auch hier stehen wir Ihnen gerne mit Rat und Tat zur Seite.

9 Vor- und Nachteile der Übertragungsverfahren

9.1 ISDN via AVM Fritz!-Data

Der Datenaustausch über AVM Fritz!-Data setzt auf beiden Seiten eine korrekt installierte und korrekt konfigurierte AVM-Fritzcard voraus. Es wird zur Datenübertragung eine normale aber kostenpflichtige Telefonverbindung (Leitungsbündelung möglich) aufgebaut. Der Weg zwischen beiden Parteien muss als Unsicher eingestuft werden, da nicht sichergestellt ist, das die Übertragung nicht "abgehört" werden kann. Zusätzliche Sicherungsmaßnahmen werden daher dringend empfohlen. Der Dienst "Fritz-Data" wird in unserem Hause nur nach Absprache und unter besonderen Bedingungen bereitgestellt. Für den Dienst

wird auf der Gegenseite Hard- und Software von AVM, mit zusätzlichen Kosten, benötigt.

9.2 FTP via ISDN Direktverbindung

Für diesen Dienst ist auf der Gegenseite (Kunde) eine ISDN-Karte sowie FTP-Clientsoftware notwendig. Per ISDN wird eine normale aber kostenpflichtige Telefonverbindung hergestellt und anhand der FTP-Software die Daten übertragen. Da auch hier nicht völlig sichergestellt werden kann, das niemand die Telefonleitung abhört, werden zusätzliche Sicherungsmaßnahmen dringend empfohlen. Der Dienst "ISDN-FTP" steht 24 h/Tag zur Verfügung. Vor der ersten Datenübertragung muss ein Benutzer/Passwort für die ISDN-Einwahl und ein Benutzer/Passwort für den FTP-Zugang eingerichtet werden.

9.3 E-Mail

Um Daten zu versenden eignet sich E-Mail aus zwei wichtigen Gründen nicht. Es funktioniert, keine Frage, ist aber absolut unsicher, da jeder (wirklich jeder) der sich ein ganz klein wenig mit dem Internet und der Technik befasst hat, dazu in der Lage ist. Dazu kommt, das E-Mail als Kommunikationsmittel gedacht und betrieben wird und für den Austausch von Daten das File Transfer Protokoll (FTP) bestimmt ist.

Wie unangenehm ist es doch auch, wenn man auf eine wichtige Mitteilung wartet und das Postfach mit Emails verstopft ist, die zum laden auf den lokalen Rechner einfach ewig dauern. Oder aber der Empfänger ist gerade nicht am Platz und eine mit Daten gefütterte Email blockiert das gesamte Postfach, so dass andere diesem Empfänger keine Emails mehr senden können.

Als Randerscheinung muss dabei noch bemerkt werden, das auf Grund der Virengefahr der Virenscanner die geladene Email erst noch prüfen muss, bevor diese auf dem Rechner freigegeben werden kann. Somit sollte E-Mail zum Datenaustausch nur im "Notfall" und dann auch nur mit geringen Dateigrößen benutzt werden. Wichtig dabei ist, das man höchstmögliche Sicherungsmaßnahmen anwendet und die komplette Email mit PGP, GnuPG oder GnuPP verschlüsselt.

9.4 FTP via Internet

Datenaustauschen über ein FTP-Server ist sicher einer der bequemsten Wege und abhängig vom Volumen und der jeweiligen Verbindung zum Internet auch einer der effektivsten. Berücksichtigt man aber, das ungeschützte Daten genau wie bei E-Mail ganz problemlos von jedem x-beliebigen Internetanwender mit mehr als Grundkenntnissen ausgelesen werden können, so muss auch hier eindringlich auf zusätzliche Sicherungsmaßnahmen hingewiesen werden. Der Datenaustausch per Internet-FTP stellt in unserem Hause die am häufigsten genutzte Möglichkeit dar. Um diese zu nutzen ist es nur notwendig einen entsprechenden Benutzer und ein Passwort einzurichten.

Kleiner Tipp: Es lohnt sich immer die Daten vor dem Übertragen zu komprimieren, beispielsweise als ZIP usw. Entsprechende Tools, die auch kostenfrei kommerziell genutzt werden dürfen finden Sie im Internet. Für die Datenübertragung selbst ist ein FTP-Client notwendig, der in fast allen Betriebssystemen standardisiert vorhanden ist. Wer lieber mit einer grafischen Oberfläche arbeiten möchte, der findet auch hier einige Tools die ebenfalls kostenlos auch kommerziell genutzt werden dürfen. Sollten Sie Probleme beim Umgang mit FTP haben, stehen wir Ihnen natürlich gerne mit Rat und Tat zur Seite.

9.5 SECURE FTP via Internet

Hinter der Abkürzung sFTP versteckt sich 'secure File Transfer Protokoll' und bedeutet nichts anderes, als das diese Form der Datenübertragung durch spezielle Maßnahmen sicherer gemacht wurde. Hier macht man sich das Netzwerkprotokoll Secure Shell (SSH) zu nutze, über dessen Weg die Daten automatisch verschlüsselt werden. Zusätzlich kann der sFTP-Server auf dem man sich einlogt anhand eines Zertifikates identifiziert werden. Die Daten befinden sich so auf sicherem Wege zu uns. SFTP setzt aber eine spezielle Software voraus, um sich mit dem Server verbinden zu können. Natürlich finden Sie auch hier im Internet kostenlose und kommerziell nutzbare Tools, wie z.B. WinSCP, PuTTY oder TeraTerm Pro. Sollten Sie Probleme beim Umgang mit sFTP haben, so stehen wir Ihnen natürlich auch hier gerne mit Rat und Tat zur Seite. Übrings: Eine zusätzliche Sicherung der Daten ist natürlich möglich, aber nicht mehr notwendig, da die Daten ja bereits auf dem Weg verschlüsselt werden.

DECODETRON setzt seit 2002 auf die Variante FTPs (FTP over SSL) und betreibt erfolgreich mit diesem Verfahren mehrere Server.

9.6 VPN Tunnel

Unter dem Kürzel VPN versteht man Virtual Private Network und wurde geschaffen, damit Beispielsweise sogenannte Homeworker von zu Hause aus auf Infrastrukturen im Unternehmen zugreifen können oder aber um Niederlassungen mit dem Hauptsitz eines Unternehmens zu verbinden. Mit VPN ist es somit möglich, von entfernter Stelle aus im Unternehmen so zu arbeiten, als würde man direkt vor dem Rechner innerhalb des Unternehmens sitzen.

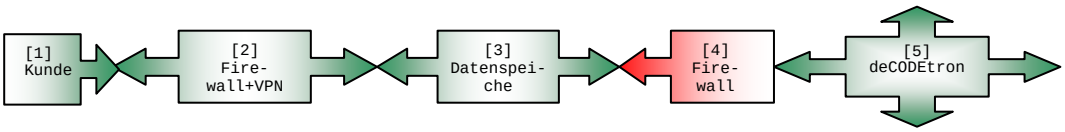
Anhand dieser Erklärung wird schon klar, das man mit VPN viel mehr kann, als eben nur Dateien von A nach B zu übertragen. Sicherlich ist das auch möglich, birgt aber auch gleich gewisse Risiken die durch aufwendigere Sicherungsmaßnahmen ausgeschlossen werden müssen. Damit verbunden ist somit auch ein erhöhter Konfigurations- und Administrationsaufwand, die beide entsprechende Wartungs- und Pflegemaßnahmen nach sich ziehen.

Um nun die Möglichkeiten für einen Datenaustausch zu ermöglichen,

muss zum einen die VPN Strecke zwischen Kunde [1] und der deCODEtron sicher aufgebaut werden. Um unerwünschte Besucher abzuwehren ist am Eingangstor zur deCODEtron eine Firewall [2] notwendig die gleichzeitig auch alles Notwendige für die VPN-Verbindung bereitstellt. Hat der Anwender sich an der VPN-Schnittstelle authentifiziert erhält er Zugriff für den weiteren Weg zum Datenspeicher [3]. Eine erneute Authentifizierung am Datenspeicher ist wiederum notwendig, um die dort vorgesehenen Rechte zu erhalten. Nun muss der Weg zum Netz der deCODEtron gegen unbefugten Zugriff gesichert werden, da sonst jeder in der Lage wäre, dort Programme auszuführen und somit auch Zugriff auf Daten anderer hätte.

Und eins ist ganz sicher: Wer VPN nutzt, will nicht das jemand unbefugtes, im schlimmsten Fall die Konkurrenz, Zugriff auf seine Daten hat.

Um aber die Daten automatisiert Verarbeiten zu können, muss die deCODEtron [5] immer direkten Zugriff auf den Datenspeicher haben und der Weg darf nur in eine Richtung der Firewall [4] gehen. Um also wirklich sicherstellen zu können, auch im Sinne aller anderen Kunden, das nichts und niemand Zugriffsmöglichkeiten auf das interne Netz der deCODEtron erhält, sind nur für die Datenübertragung drei zusätzliche Rechner notwendig die neben der eigentlichen Hardware auch Kosten für Installation, Konfiguration, Administration sowie Pflege und Wartung aufwerfen. Alles in allem fallen damit nicht unerhebliche Kosten an, die im Vorfeld unbedingt abgestimmt werden müssen.



10 Sichere Passworte

10.1 Grundsätzliches zu sicheren Passworten

Die Absicherung Ihrer Daten mit Passworten dient Ihrer und der Sicherheit Ihres Unternehmens. Dabei bleibt zu bedenken, das grundsätzlich nichts wirklich zu 100 % sicher sein kann. Zu jedem Schloss kann man auch einen Nachschlüssel erstellen oder einen Dietrich benutzen. Doch je größer und komplizierter das Schloss ist, desto schwerer ist es auch, es zu knacken. Das gleiche gilt auch für Passworte.

10.2 Mindestanforderungen an gute Passwörter

Die Länge eines Passwortes spielt immer eine ganz große Rolle. Grundsätzlich gilt, je länger ein Passwort ist, desto aufwendiger

ist es auch, dieses zu knacken. Simple und kurze Passworte wie z.B. "Auto" finden Kiddis heute schon zwischen der Schule und den Hausaufgaben raus. Damit wird klar, das Passworte niemals aus logischen Worten bestehen sollten.

Quasi Worte, wie sie auch im Wörterbuch stehen, aber auch Vor- und Nachnamen, Firmennamen, Produktnamen, Emailadressen, Geburtstage als einfache Zahlenfolge, usw. Eben Begriffe des täglichen Lebens sollten unbedingt vermieden werden.

Als Passwort ganz verpönt sollte in jedem Fall das Wort "Passwort" selbst sein. Das Wort selbst zu benutzen ist wahrscheinlich genauso alt wie die eigentlich Erfindung des Passwortes und wird von so ziemlich jedem Hackerlehrling einfach mal zu ganz am Anfang probiert werden.

Aber auch logische Folgen von Buchstaben oder Zahlen sind kein guter Trick mehr. Sicher, einfach zu merken ist es dann schon, aber auch genauso einfach herauszufinden. Entsprechende winzig kleine Programme die man ganz ungestört aus dem Internet bekommen kann, arbeiten nach der sogenannten "Brute Force-Attack", mit der Sie dem Passwort auf die Spur kommen. Das ist schlicht das Ausprobieren aller möglichen Kombinationen von Buchstaben, Zahlen und Sonderzeichen. Somit sind Passworte wie AAA, ABC, abc, Abc, 123, 111, 000 einfach sinnlos, da auch diese schneller gefunden werden, als manchem lieb sein dürfte.

Ach ja, nicht das ich es vergesse, aber wer sein Passwort aufschreibt und als Gelbe-Klebe-Notiz an den Bildschirm pappt, oder aber mit Klebefilm unter die Tastatur oder das Mauspad klebt, oder in der Schublade sammelt, oder an die Unterseite der Kaffeetasse anhaftet, oder auch direkt auf dem Rechner abspeichert, der darf sich natürlich auch nicht wundern, wenn alle Welt sein kompliziertes, langes und doch nicht sicheres Passwort kennt. :-)

Dabei geht das doch wirklich so einfach, sich auch lange und komplizierte Passworte zu hauf zu merken...

10.3 Komplizierte Passworte die man sich merken kann

Generell sollten Passwörter also schwer zu erraten, aber für einen selbst immer und jederzeit leicht merkbar sein.

Am besten eignen sich lange und kryptische Passworte. Unter kryptisch versteht man dabei die Kombination aus Buchstaben (ABC...XYZ, abc...xyz), aus Zahlen (012...789) und aus Sonderzeichen (!"§$...%&/=). So entstehen Passworte, deren Sicherheit sich nicht schämen muss. Klar, so was wie JK!156C/g5ioc+Tc.gic7t/&Tc87t können sich auch ausgebuffte Profis nur durch stumpfes auswendig lernen merken. Braucht man es dann eine Weile nicht, ist es womöglich ver-

gessen und die damit gesicherten Daten futsch. Alternativen müssen her.

10.4 Tipps & Tricks und wie es einfach geht

Kryptische Passworte bestehen also aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen in offensichtlich unlogischer Reihenfolge. Da solche Wortbildungen wirklich schwer zu merken sind, gibt es für sichere Passworte zwei Möglichkeiten:

10.4.1 Die Satz-Variante

Denken Sie sich doch einen Satz aus und bilden aus den jeweiligen Anfangsbuchstaben ihr ganz persönliches Passwort. Diesen werden Sie sich dann ganz bestimmt sehr viel leichter merken können und sich so immer an ihr Passwort erinnern.

Ein Satz-Beispiel: **MTieA4x4!**

Das Passwort wurde aus dem Satz "**M**ein **T**raum **i**st **e**in **A**udi **4x4!**" gebildet und enthält so eine fast perfekte Zusammensetzung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen für ein Passwort.

Und damit es noch Sicherer wird, hier noch ein längeres Satz-Beispiel:

UUiES2004wdsugUdJ!

Unser **U**rlaub **i**n **E**l **S**alvador **2004** **w**ar **d**ie **s**chönste **u**nd **g**lücklichste **Z**eit **d**es **J**ahres**!**

Das Passwort sieht beeindruckend kompliziert aus, oder? Es ist dabei auch schon viel sicherer und wenn man den Satz dazu kennt, doch sehr einfach zu merken.

Die gerade genannten Beispiele sollten Sie nun auch nur als Beispiel nehmen und nicht als Passwort genauso übernehmen. Aber das war ja auch noch nicht alles, denn es gibt noch eine Möglichkeit...

10.4.2 Die Scriptkiddie-Variante

Bei der Scriptkiddie-Variante werden Buchstaben durch Zahlen oder durch Sonderzeichen ersetzt, die diesen optisch irgendwie ähnlich sind. So wird zum Beispiel aus dem A eine 4 und aus dem E eine 3 (Spiegelverkehrt) und aus dem M ein /\/\ (Slash + Backslash + Slash + Backslash).

Aus der folgenden Tabelle können Sie die Kombinationen entnehmen und so auch ganz normale Worte als Passwort umsetzen.

A = 4 od. @	B = 8	C = (	D = |)	E = 3
F =	G = 6 od. &	H = |-|	I = 1	J =
K = |<	L =	M = /\/\	N = ||	O = 0 (null)
P =	Q =	R =	S = 5	T = 7
U =	V = \/	W = \/\/	X = +	Y =
Z = 2				

So entstehen auch aus ganz einfachen Worten wie das 12 Zeichen lange Wort "GABELSTAPLER" prima Passworte, die verschlüsselt sich als "6@83L574PL3R" lesen. Kombiniert man nun noch das Ganze mit Groß- und Kleinschreibung steigert sich der Sicherheitsfaktor erneut.

Auch eine Kombination aus der "Satz-Methode" mit der "Scriptkiddie-Methode" wäre denkbar und würde den Sicherheitsaspekt wieder weit nach oben setzen.

Aber ich gebe zu, das die Kombination beider Varianten sehr schwer zu handhaben ist, besonders dann, wenn man das Passwort häufig eingeben muss.

Versuchen Sie doch nun einmal zur Übung den folgenden Satz nach der Scriptkiddie-Variante zu "übersetzen":

/\/\31n P@55w0r7 50ll w1rkl1ch 51ch3r und 53hr 5chw3r h3r@u5zuf1nd3n 531n

Die Lösung dazu finden Sie, wenn Sie den Bereich zwischen den beiden Linien mit gedrückter linker Maustaste markieren.

Mein Passwort soll wirklich sicher und sehr schwer herauszufinden sein

---

10.5 Faustformel

Als Faustformel sollten sie immer das ABC für sichere Passworte beachten:

A. **Niemals aufschreiben** (und natürlich auch keinem anderen sagen)

B. So **lang** wie nur irgendwie möglich

C. So **kryptisch** wie nur irgendwie möglich

11 Aufbereiten der Daten

11.1 Welche Dateiformate dürfen nach der GDPdU verwendet werden?

Da Ihre Daten im Originaldatenstrom gehalten werden, müssen Sie um die Vorschriften der Finanzverwaltung zu erfüllen, eines der folgenden Formate nutzen:

- ASCII feste Satzlänge
- ASCII Delimited (einschließlich Kommagetrennter Werte)
- EBCDIC feste Satzlänge
- EBCDIC Dateien mit variabler Länge
- Excel (auch ältere Versionen)
- Access (auch ältere Versionen)
- dBASE
- Lotus 123
- ASCII-Druckdateien (plus Info für Struktur und Datenelemente etc.)
- Dateien von SAP/AIS
- Konvertieren
- von AS/400 Datensatzbeschreibungen (FDF-Dateien erstellt von PC support/400) in RDE-Datensatzbeschreibung
- Import durch ODBC-Schnittstelle

Nicht erkennbare Dateiformate müssen in lesbare Formate konvertiert werden.

Bitte beachten Sie in jedem Fall die aktuellen Vorschriften der Finanzverwaltung !

11.2 Inhalte der Daten

Für die eigentliche Verarbeitung in unserem Hause ist es wichtig, das die Daten grundlegende Informationen, wie im folgenden Beispiel genannt, enthalten:

- Druckdaten inkl. der Zeilen- und Seitenvorschübe
- um die korrekte Trennung der Dokumente übernehmen zu können.
- Mandantennummer, Buchungskreis, Geschäftsjahr, Seitenzahl, Datum, Kundennummer oder Belegnummer,
- usw. um für die Rechercheapplikation entsprechende Suchdaten in die Datenbank übernehmen zu können.