

Anleitung zur Verschlüsselung von Dokumenten

Vertrauliche Daten auf Datenträgern und in E-Mails

18.1.10 Adrian Meyer

Ausgangslage

Auf USB-Sticks, externen Festplatten, CDs und anderen Datenträgern haben wir oft Dateien (Texte, Tabellen, Fotos usw.) mit vertraulichem Inhalt, ohne dass wir besondere Vorkehrungen zum Schutz treffen. Diese Datenträger können verloren gehen oder in unbefugte Hände geraten.

E-Mails sind wie offene Postkarten; sie können durch alle Personen, die Zugang zum Benutzerkonto der beteiligten Computer haben, durch Systemadministratoren und versehentliche Empfänger usw. eingesehen werden. E-Mail ist aber im Austausch der Mitarbeitenden einer Sonderschule nicht mehr wegzudenken.

Gesucht ist ein einfaches Verfahren, Dateien und Mitteilungen für Unbefugte zuverlässig unlesbar zu machen. Es braucht eine Verschlüsselung. Lediglich ein Kennwortschutz genügt nicht.

Massnahmen

1. E-Mails dürfen in Betreff und Text keine Personen- und Ortsnamen ausser der Adressaten und Absender aufweisen. Umschreibungen, die für Dritte keine Rückschlüsse zulassen, können verwendet werden: 'Schülerbericht', 'Besprechung vom 1.4.00', 'zum Schüler, über den wir gestern gesprochen haben'. – Initialen und Abkürzungen analog 'am vom SHC' sind nicht sicher.
2. Sensible Daten werden in einer Datei gespeichert, und diese wird verschlüsselt versandt.

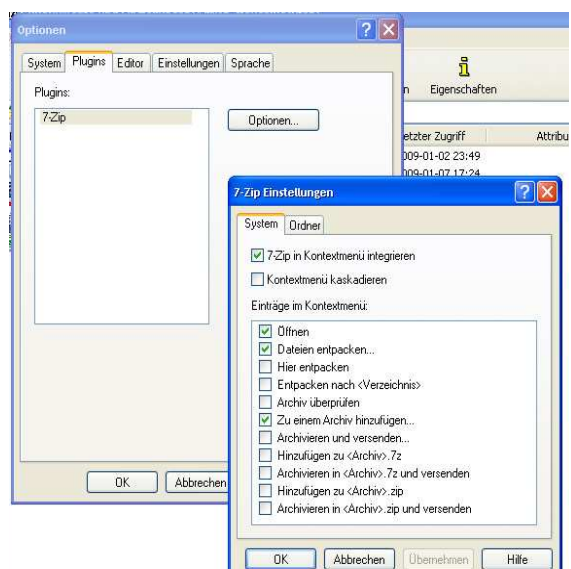
Software installieren und einrichten

Ein einfaches Verfahren zur Verschlüsselung bieten Packprogramme wie WinZip oder 7-Zip. Wir verwenden 7-Zip, eine freie Software, die ohne Entgelt benutzt werden darf. Sie kann von der Webseite www.7-zip.org heruntergeladen werden. Die Installation erfolgt in wenigen Sekunden.

Einstellungen (Voraussetzung ist Anmeldung in Windows mit Administratorenrechten): 7-Zip starten. Im Menu 'Extras' – 'Optionen....' im Reiter 'Plugins' 'Optionen' wählen und folgende Einstellungen vornehmen:

1. '7-Zip im Kontextmenu integrieren' mit Häkchen versehen
2. 'Öffnen', 'Dateien entpacken', 'Zu einem Archiv hinzufügen' mit je einem Häkchen versehen, die anderen Optionen nicht.
3. 'OK' anklicken, nächstes Fenster auch mit 'OK' schliessen

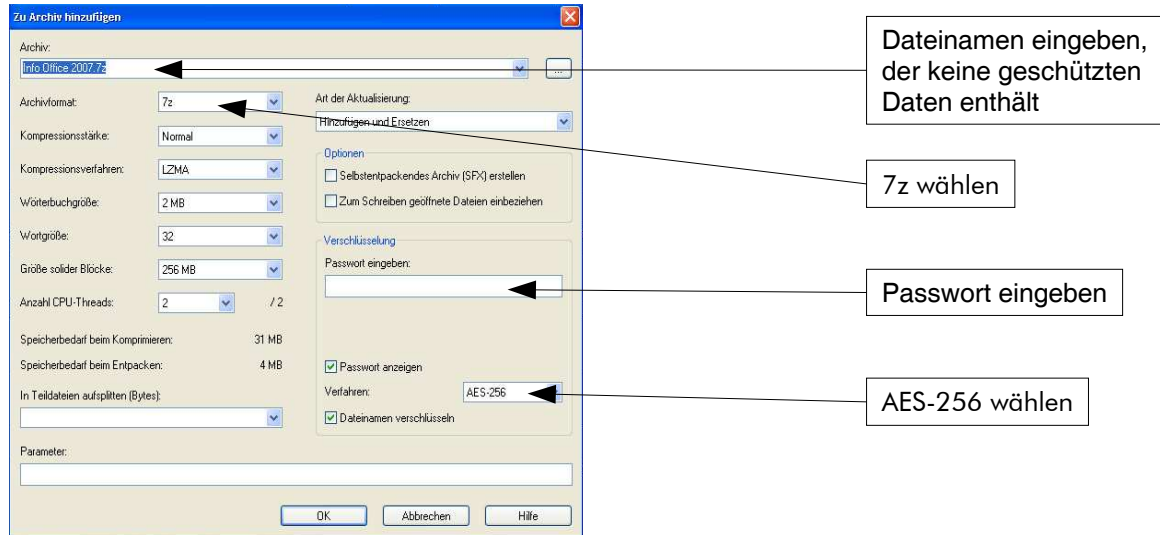
Kontrolle: Das Kontextmenu bei einem Rechtsklick auf eine Datei muss die Einträge 'Öffnen' (nicht fett), 'Dateien entpacken.....' und 'zu einem Archiv hinzufügen.....' enthalten.



Software anwenden

Verschlüsseln einer Datei / mehrerer Dateien

1. Rechtsklick auf die gewünschten und markierten Dateien. Im Fenster, das sich öffnet, wählen 'zu einem Archiv hinzufügen...'
2. Ein neues Fenster öffnet sich. Die vorgegebenen Einstellungen können belassen werden.



Einen geeigneten Dateinamen (ohne geschützte Daten wie Namen) und ein Passwort eingeben – und sich merken – dann OK drücken. Die verschlüsselte und komprimierte Datei wird im selben Ordner wie die Originaldatei erstellt.

3. Die verschlüsselte Datei kann auf einen USB-Stick kopiert, auf eine CD gebrannt werden oder wie eine andere an ein Mail angehängt werden. Im Mail dürfen keine geschützten Daten genannt werden.
4. Das Passwort auf einem anderen Weg als den Datenträger übermitteln: SMS (Achtung: Gross-i und klein-L sowie 0 und O können verwechselt werden), Post, Telefon, persönlich.

Exkurs: Datenträger

Mit dem beschriebenen Verfahren können auch Dateien und Ordner auf Datenträgern (Festplatten, USB-Sticks usw.) verschlüsselt werden.

Empfangen und öffnen von verschlüsselten Dateien

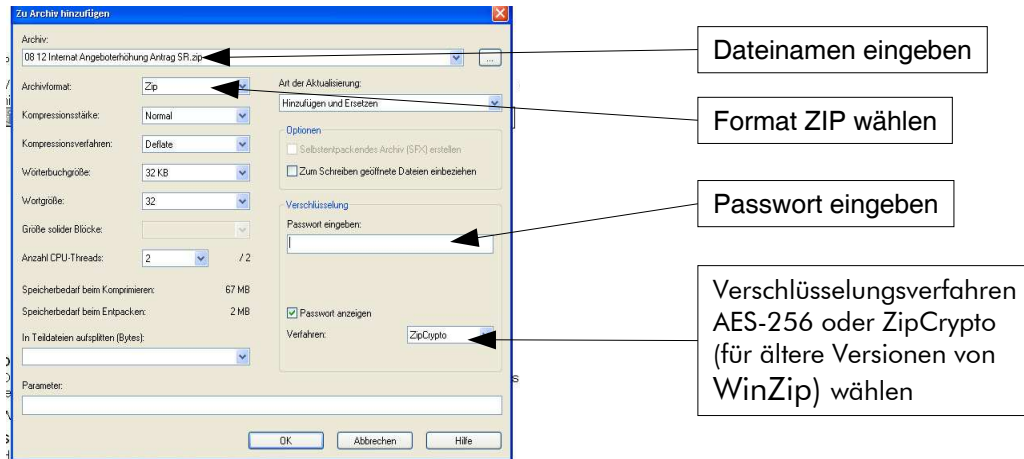
1. Die 7zip-Datei im Mail-Anhang speichern.
2. Doppelklick auf die Datei. Ein kleines Fenster mit der Fragen nach dem Passwort ('Kennworteingabe') erscheint. Passwort eingeben und auf OK drücken.
3. Dateiname anklicken, dann auf 'entpacken'. Die Datei wird entschlüsselt im selben Ordner gespeichert und kann nun normal geöffnet und bearbeitet werden.



Wenn der Empfänger kein 7-Zip hat

Verschlüsselte Dateien können auch an Personen, die nicht über 7-Zip verfügen gesandt werden. WinZip Version 12 und auch andere (PowerArchiver, WinRAR) können diese Dateien öffnen.

Bei älteren Versionen von WinZip und anderen die Dateien im Format Winzip (.zip) speichern. Kompression und Verschlüsselung sind dann nicht so gut.



Solche Dateien können mit fast allen Packprogrammen geöffnet werden. Der Umgang mit dem Passwort bleibt wie oben beschrieben.

Organisation Passwörter

Passwörter werden per SMS oder auf Papier versandt oder telefonisch übermittelt und können für ein Quartal oder Semester gültig sein. Ein Bereich (oder das ganze Schulheim) kann ein Passwort für alle Mitarbeitenden verwenden.

Regeln für sichere Passwörter

- Acht Zeichen sind das Minimum, besser sind 10 Zeichen (Empfehlung Datenschutzbeauftragter Kanton Zürich)
- Mit Gross- und Kleinbuchstaben (Gross-i und klein-L sowie 0 und O sind ähnlich)
- Enthalten mindestens eine Ziffer
- Enthalten Sonderzeichen (z.B. *ç&%+).
- Ohne eine persönliche Angaben wie Namen, Geburtsdaten oder Telefonnummern
- Ohne Wörter, die in einem Wörterbuch stehen

Gute Passwörter sind oft schwierig zu merken. Ein Phantasie-Passwort kann dem abhelfen:

1. Die Anfangsbuchstaben aus einem geläufigen Satz verwenden. Beispiel: Räuber Hotzenplotz fängt im Walde rote Füchse. Das gibt dann: RhfiWrF.
2. Ein Sonderzeichen # dazu, dann sind es 8 Zeichen: RhfiWrF#
3. Die erste Telefonnummer von zu Hause aus Ihrer Kindheit anhängen: RHfiWrF#452390

Weitere Möglichkeiten

- Zeichen benutzen, die entweder gleich ausgesprochen werden (c = see, u = you, 4 = for, @ = at)
- immer die Taste, die z.B. links über der ursprünglichen Taste benutzen,
- Zeichen nutzen, die einander ähneln, z.B. (1 = l = | = I; a = @; 3 = W = E = B; 4 = A)

Schlussbemerkungen

Das hier vorgestellte Modell ist ein Baustein zu einem verantwortungsbewussten Umgang mit sensiblen Daten. Die Massnahmen sind einfach durchführbar und wirksam. Je nach Betrieb sollen sie variiert und ergänzt werden.

Beim Datenschutzbeauftragten des Kantons Zürich lassen sich Passwörter online auf ihre Eignung prüfen: <https://passwortcheck.datenschutz.ch/check.php?lang=de>

Auf dessen Webseite finden sich weitere Informationen und Hilfen zum Datenschutz: www.dsb.zh.ch

Die Post hat ein kostenpflichtiges Angebot zum verschlüsselten Mailversand mit Empfangsbestätigungen und Zertifikaten: IncaMail www.incamail.ch

Herzlichen Dank an Oliver Wyler, IT Risk Manager und Kollege im Vorstand der Rudolf Steiner Schule Winterthur, für seine fachliche Unterstützung

7-zip downloaden und installieren

1. www.7-zip.org öffnen

Welcome to the 7-Zip Home!

7-Zip is a file archiver with a high compression ratio.

Download 7-Zip 4.65 (2009-02-03) for Windows:

Link	Type	Windows	Size
Download	.exe	32-bit	1 MB
Download	.msi	x64	1 MB

Download 7-Zip 9.16 beta (2010-09-08) for Windows:

Link	Type	Windows	Size
Download	.exe	32-bit	1 MB
Download	.msi	x64	1 MB

The download links above redirect you to download pages on SourceForge.net

License

7-Zip is **open source** software. Most of the source code is under the **GNU LGPL** license. The unRAR code is under a mixed license: GNU LGPL + unRAR restrictions. Check license information here: [7-Zip license](#).

You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

The main features of 7-Zip

- High compression ratio in new [7z format](#) with **LZMA** compression
- Supported formats:
 - Packing / unpacking: 7z, ZIP, GZIP, BZIP2 and TAR
 - Unpacking only: ARJ, CAB, CHM, CPIO, DEB, DMG, HFS, ISO, LZH, LZMA, MSI, NSIS, RAR, RPM, UDF, WIM, XAR and Z.
- For ZIP and GZIP formats, **7-Zip** provides a compression ratio that is 2-10 % better than the ratio provided by PKZip and WinZip
- Strong AES-256 encryption in 7z and ZIP formats
- Self-extracting capability for 7z format
- Integration with Windows Shell
- Powerful File Manager
- Powerful command line version
- Plugin for FAR Manager
- Localizations for 74 languages

7-Zip File Manager

File Edit View Favorites Tools Help

Add Extract Test Copy Move Delete Info

C:\Program Files\7-Zip\

2. Download anklicken

Welcome to the 7-Zip Home!

7-Zip is a file archiver with a high compression ratio.

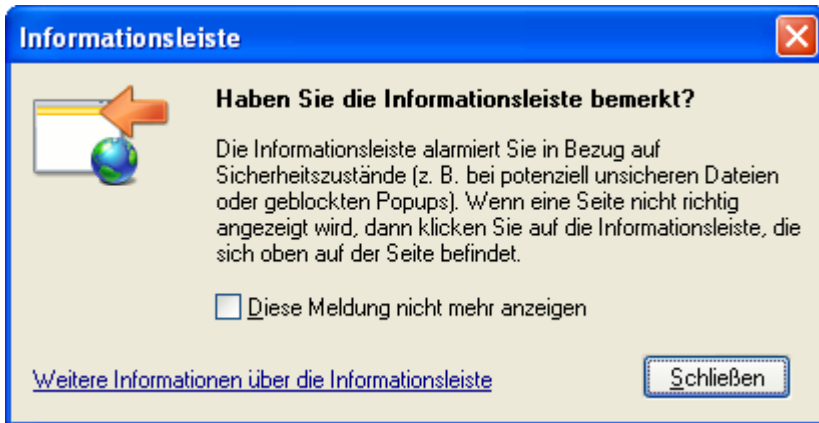
Download 7-Zip 4.65 (2009-02-03) for Windows:

Link	Type	Windows	Size
Download	.exe	32-bit	1 MB
Download	.msi	x64	1 MB

Download 7-Zip 9.16 beta (2010-09-08) for Windows:

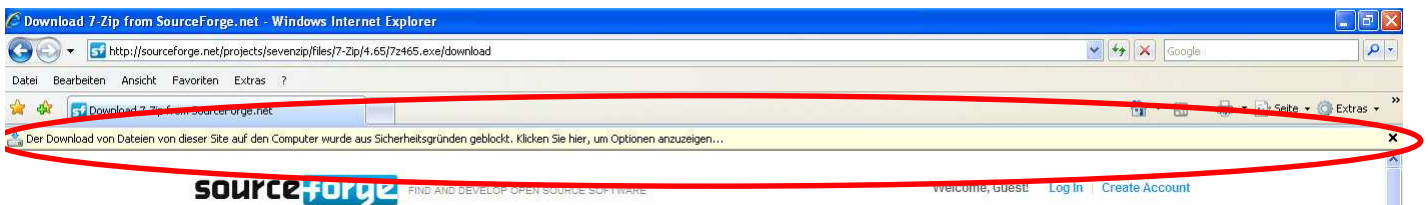
Link	Type	Windows	Size
Download	.exe	32-bit	1 MB
Download	.msi	x64	1 MB

3. Warten bis folgendes Fenster erscheint

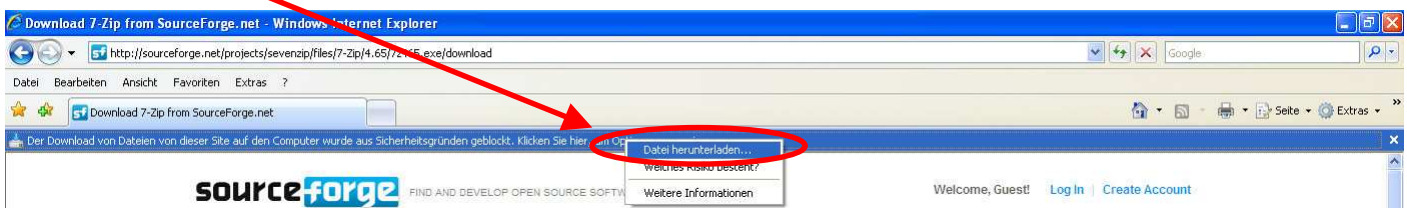


4. Schliessen anklicken.

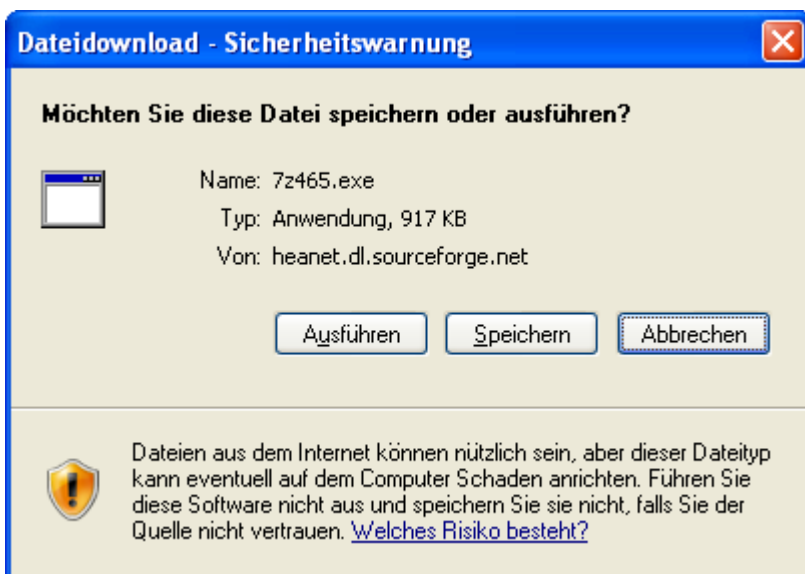
5. Diese Linie anklicken.



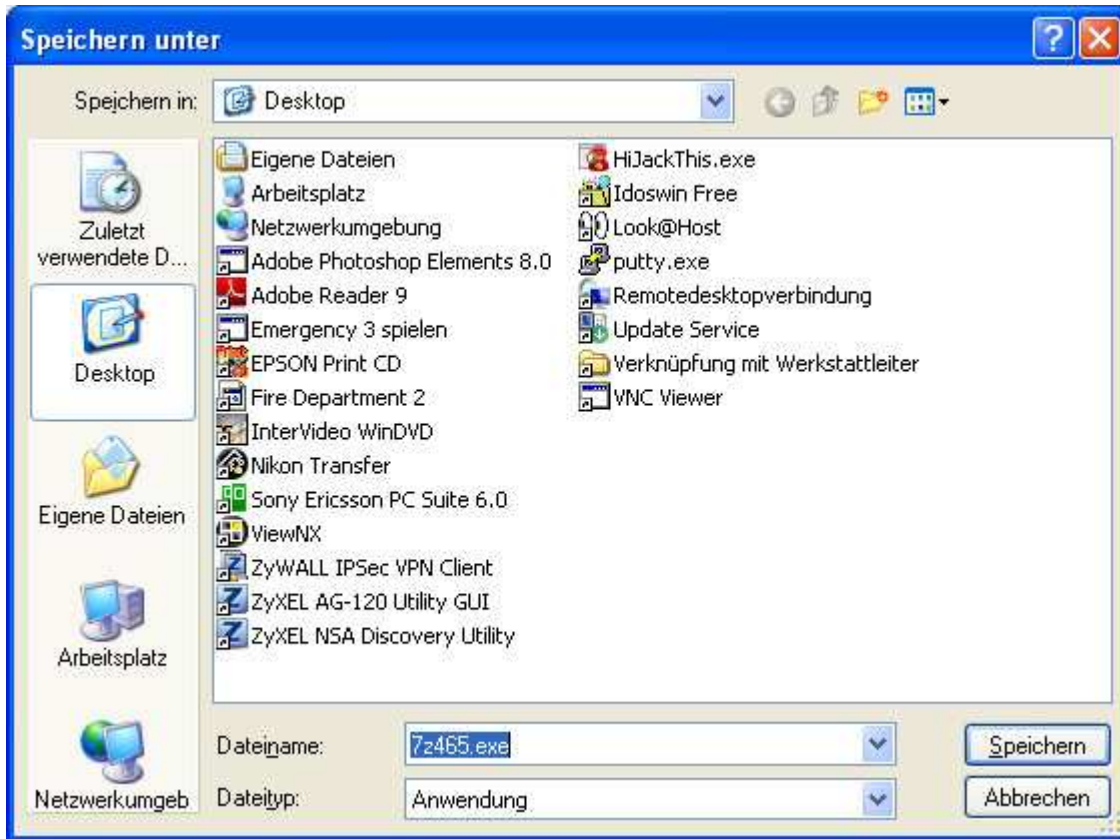
6. Datei herunterladen anklicken.



7. Bei nächsten Fenster auf speichern klicken.

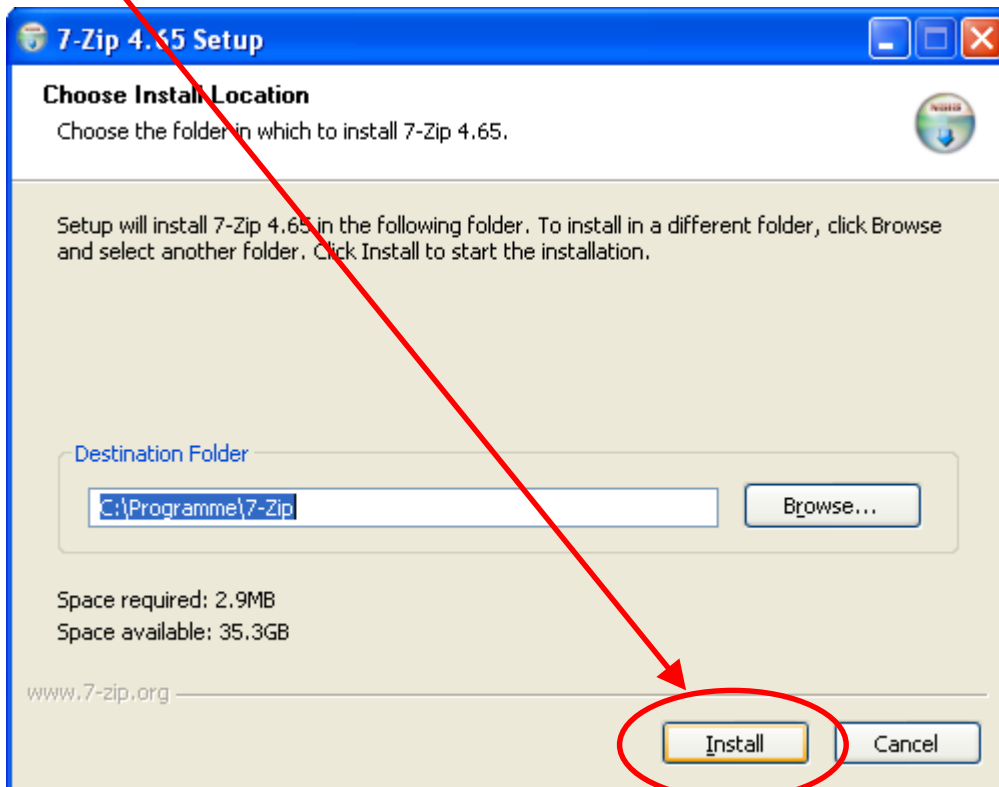


8. Irgendwo speichern, wo man es auch wieder findet.

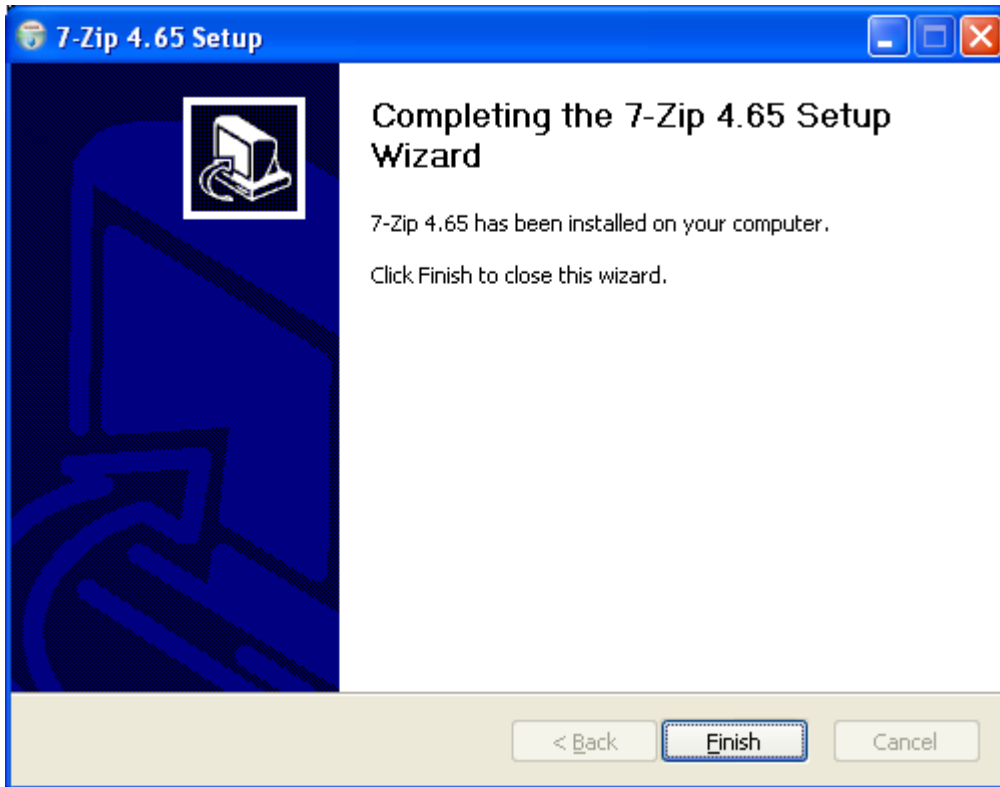


9. Ausführen anklicken

10. Install anklicken



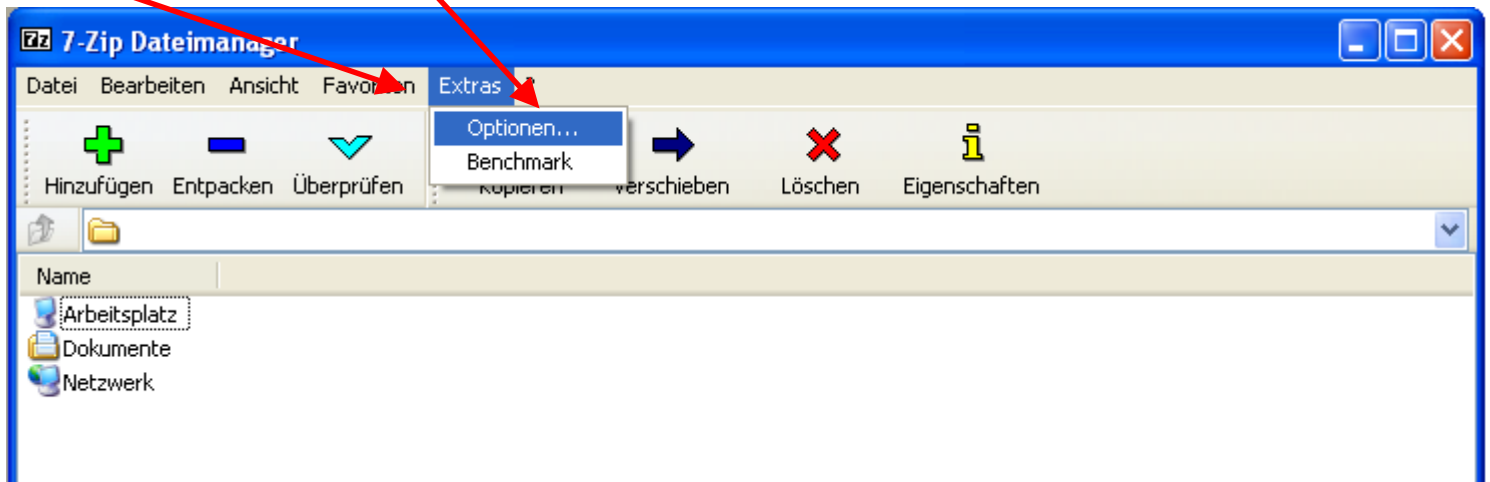
11. Finsih anklicken



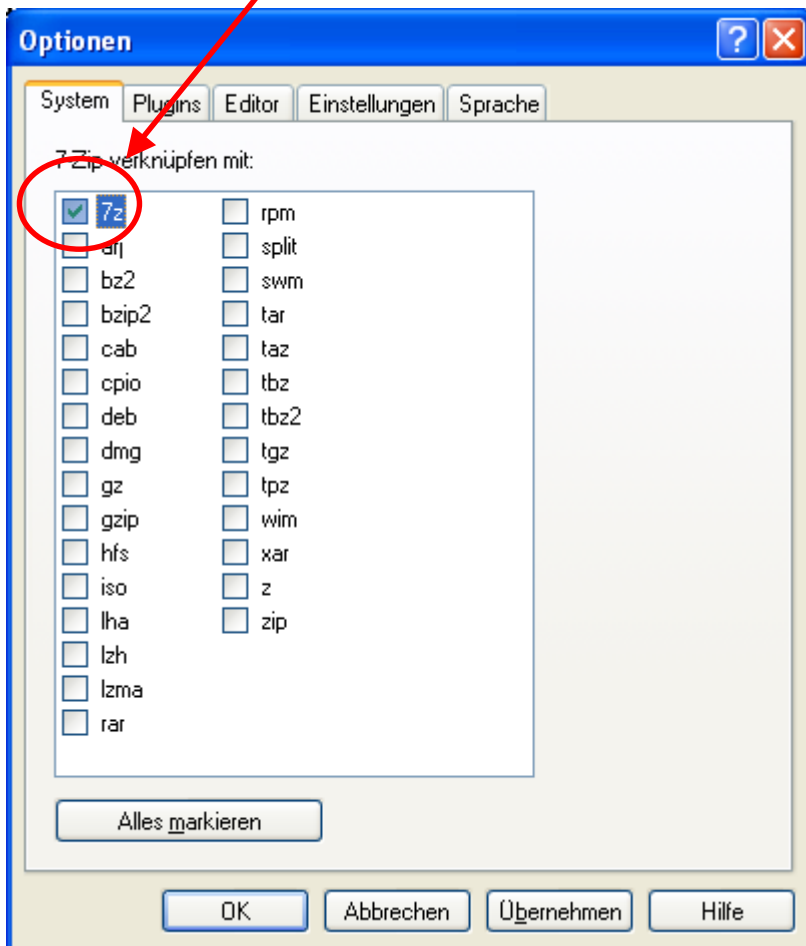
Nun kann muss man das Programm noch einrichten.

7-zip einrichten

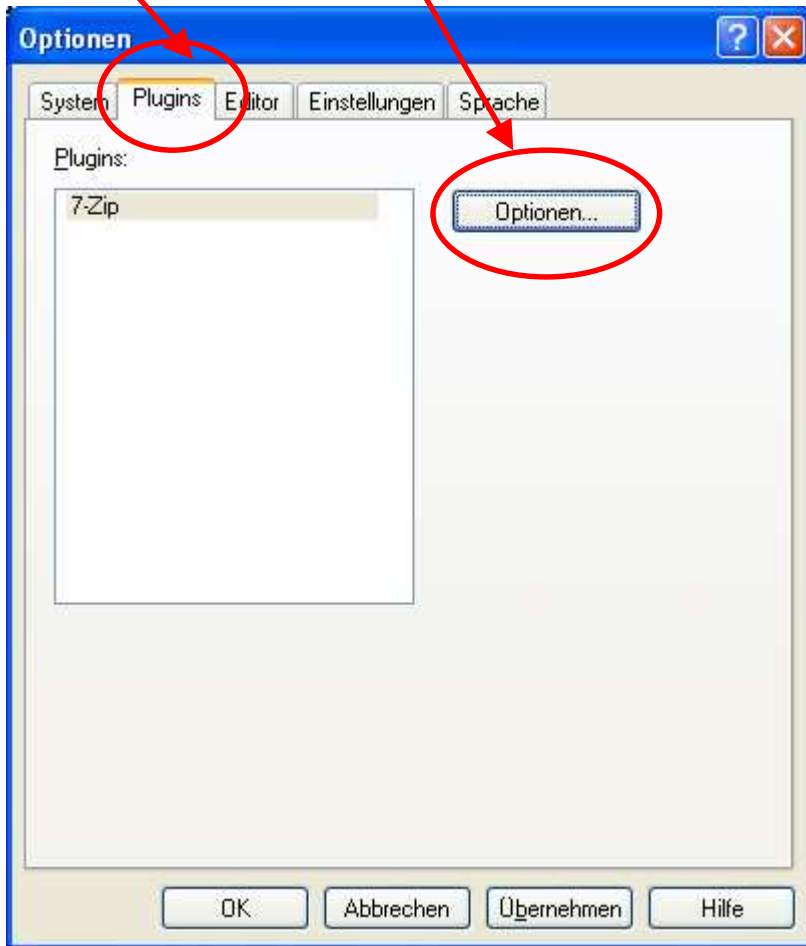
1. 7-zip unter Start / Alle Programme / 7-Zip / 7- Zip File Manager starten
2. Extras und danach Optionen anklicken



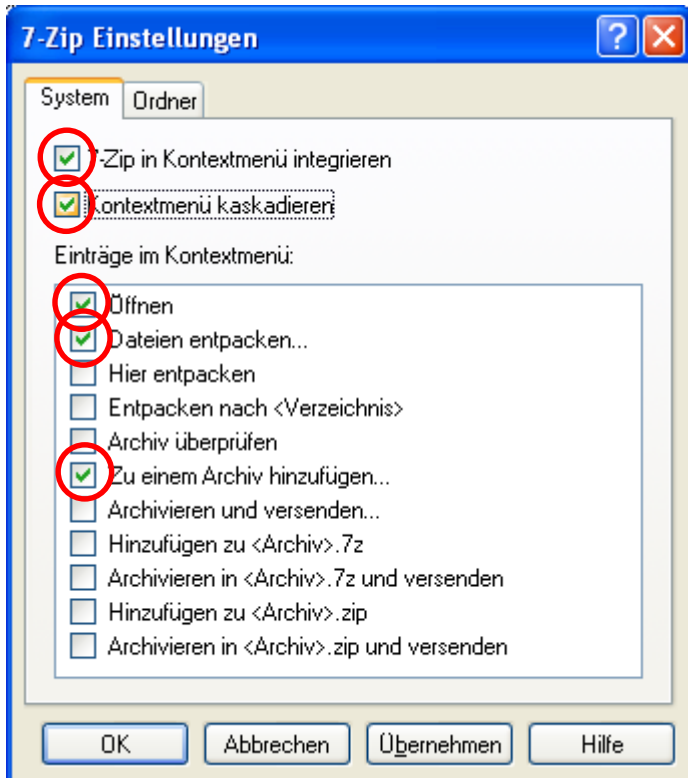
3. 7z mit einem Häkchen versehen



4. Plugins und danach Optionen anklicken



5. Folgende Häkchen stehen lassen alle andere entfernen.



6. Mit Klick auf OK bestätigen

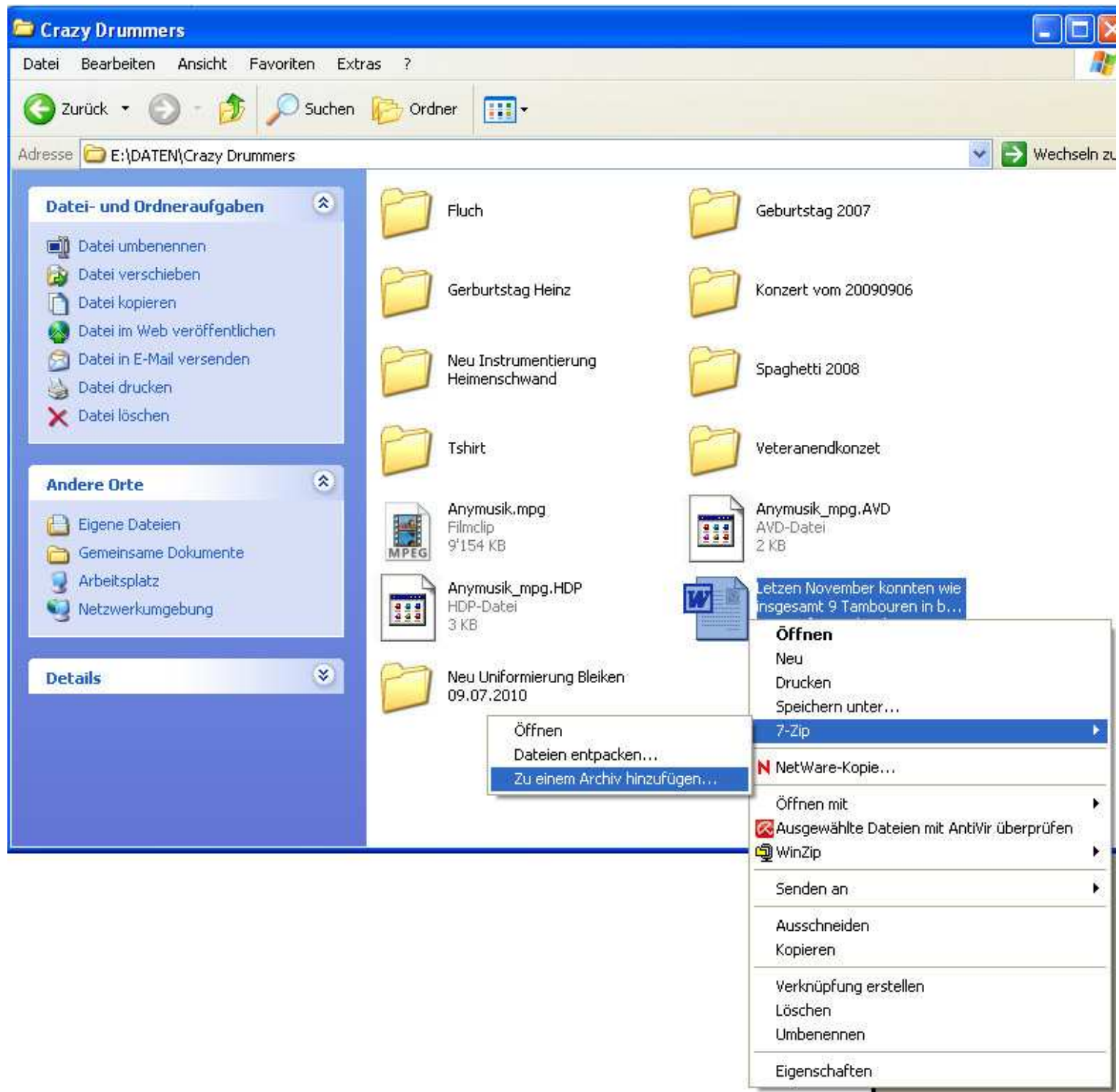
7. Noch einmal auf OK klicken

8. 7-Zip Dateimanager schliessen

Nun kann die Software verwendet werden.

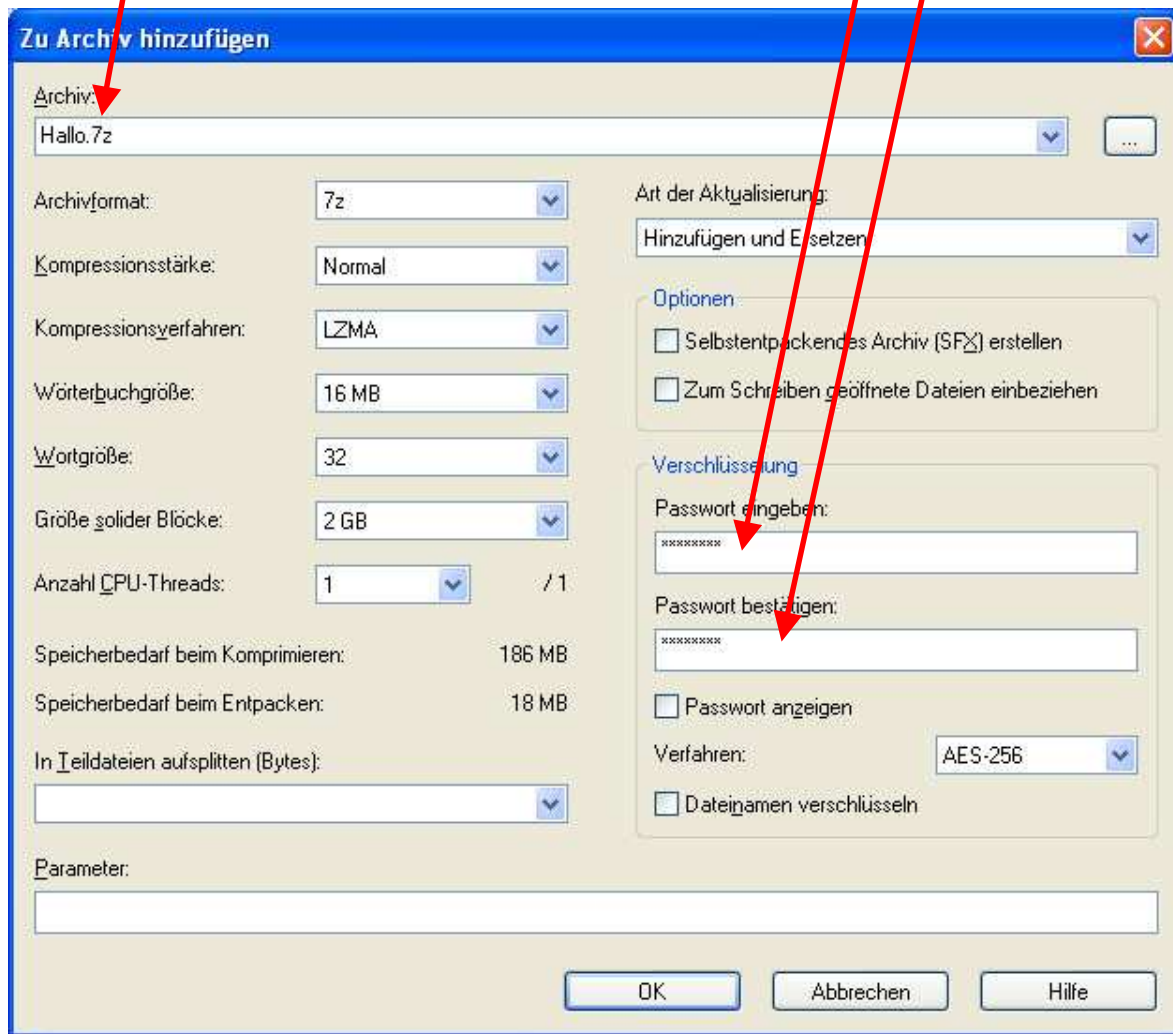
7-zip verwenden

1. Die Datei welche man verschlüsseln möchte mit der rechten Maustaste anklicken.



2. 7-zip / Zu einem Archiv hinzufügen anklicken.

3. Namen der neuen verschlüsselten Datei angeben und Passwort vergeben.



Namen: Keine Personen und Ortsnamen
Keine Angaben über den Inhalt
Keine Umschreibungen welche Rückschlüsse zulassen

Gilt auch für Mail - Betreff

Passwort: Min. 8 Stellen besser 10
Vorsicht bei l (kleines L) und I (groses i) oder 0 (Zahl Null) und O (groses o)
Muss ein Sonderzeichen wie %&+*ç und eine Zahl enthalten
Ohne persönliche Angaben wie Namen, Geburtstag oder Telefonnummern
Ohne Wörter welche in einem Wörterbuch, egal welcher Sprache stehen
Auf anderem Weg übermitteln (SMS, auf Papier oder mündlich etc.)

Typ zur Passwortvergabe:

Merken Sie sich einen Satz und nehmen Sie die jeweiligen Anfangsbuchstaben.

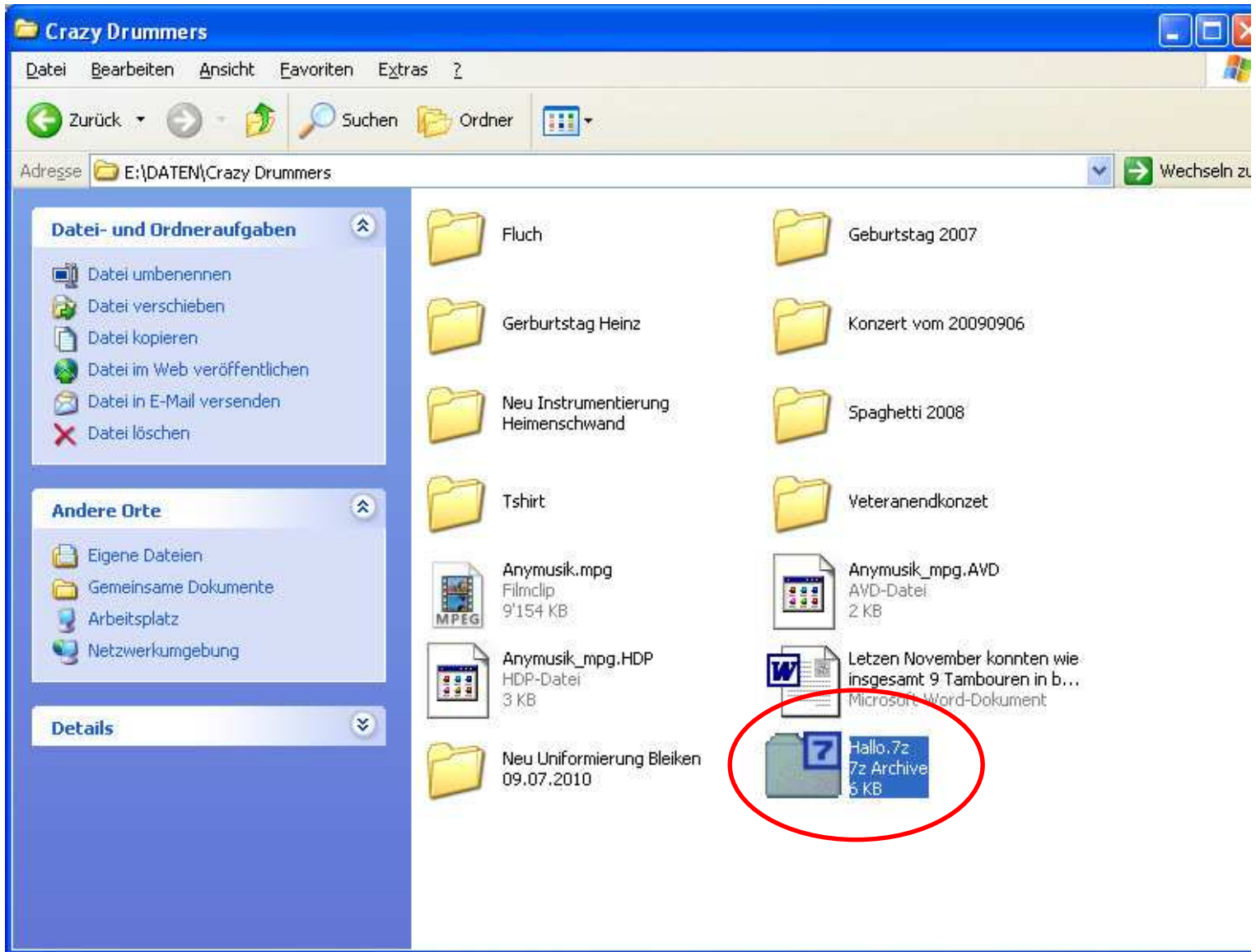
Beispiel:

Die Firma domatech AG ist unsere EDV Firma aus 7000 Chur

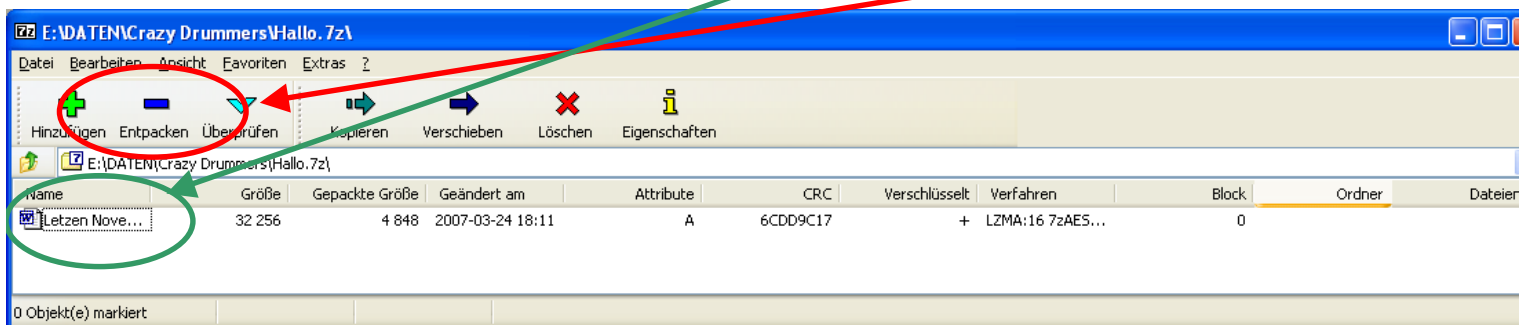
D f d A i u E F a 7 C

Nun kann die verschlüsselte Datei versendet werden.

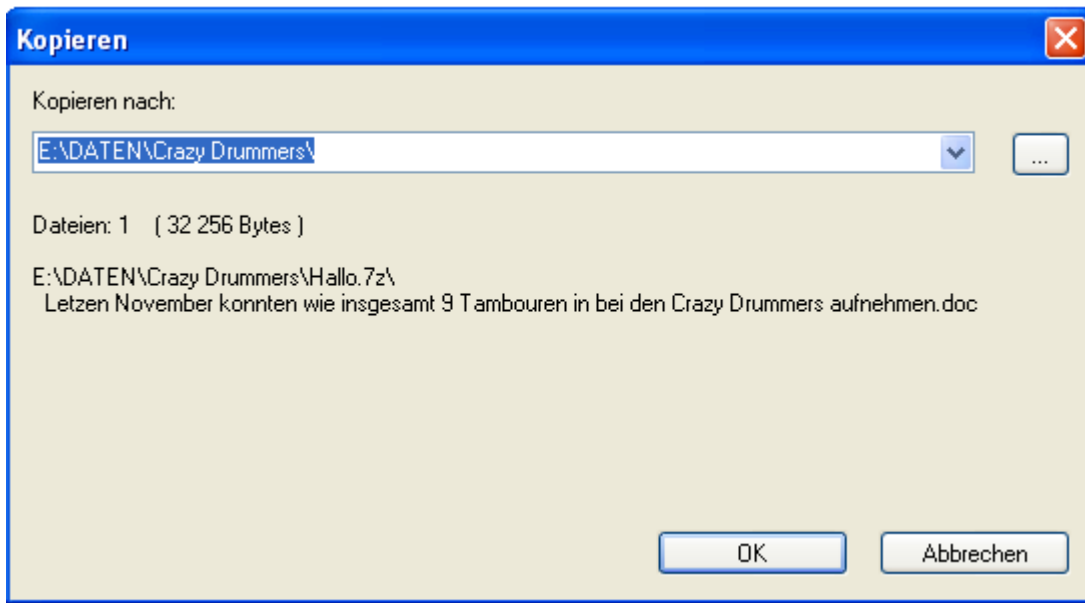
1. Der Empfänger öffnet durch doppelklicken die Datei.



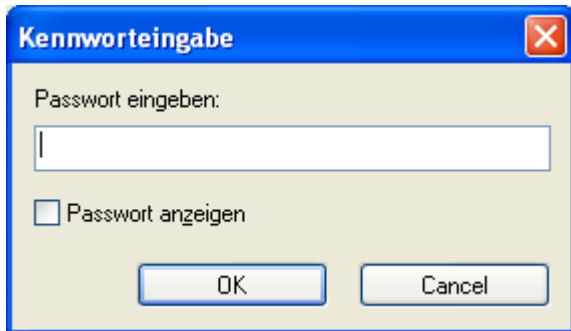
2. Nun sieht er den Originalnamen und kann die Datei anklicken und auf entpacken klicken.



3. Speicherort der entpackten Originaldatei angeben



4. Passwort eingeben.



Nach der Eingabe vom Passwort wird die Datei am Speicherort normal zur Verfügung stehen.