Inhaltsverzeichnis

Verschlüsselung

Definition: „Verschlüsselung nennt man den Vorgang, bei dem ein „Klartext“ mit Hilfe eines Verschlüsselungsverfahrens (Algorithmus) in einen „Geheimtext“ umgewandelt wird. Als Parameter des Verschlüsselungsverfahrens werden ein oder mehrere Schlüssel verwendet.“ [**Wikipedia – die freie Enzyklopädie**]

Ziel der Verschlüsselung ist das Verhindern des nicht berechtigten Mitlesens von Daten, das Schützen der Daten vor unerkannten Änderungen und das Überprüfen, ob die Daten von einem bestimmten Benutzer stammen.

Dabei unterscheidet man 2 Arten von Verschlüsselungsalgorithmen: Asymmetrisch und symmetrische Verschlüsselung. Auf diese beiden Arten soll im Folgenden etwas genauer eingegangen werden.

Asymmetrische Verschlüsselung

Die asymmetrische Verschlüsselung verwendet zwei komplementäre (sich ergänzende) Schlüssel. Ein Schlüssel – der öffentliche Schlüssel (auch Public Key genannt) – wird für das Verschlüsseln und ein anderer – der private Schlüssel (Private Key) zum Entschlüsseln genutzt.

Bei der asymmetrischen Verschlüsselung gibt es immer zwei sich ergänzende Schlüssel. Ein Schlüssel - der Public Key - für das Verschlüsseln einer Nachricht, ein anderer - der Private Key - für das Entschlüsseln. Beide Schlüssel zusammen bilden ein Schlüsselpaar.

Das Besondere an der Sache ist, dass aus dem einem Schlüssel der dazugehörige zweite Schlüssel nicht so leicht erraten oder berechnet werden kann. Dadurch kann man einen Schlüssel des Schlüsselpaares für jedermann öffentlich zugänglich machen. Daher auch die Bezeichnung Public Key.

Stellen Sie sich am besten einen Tresor mit Schnappschloss vor. Sie können etwas einschließen, weil der Tresor sich automatisch schließt, wenn die Tür ins Schloss fällt. Zum Öffnen benötigen Sie allerdings einen Schlüssel. Wie bei dem Tresor kann also jeder mit dem Public Key etwas einschließen. Weil aber nur der Empfänger über den geheimen, den Private Key verfügt, kann nur er die Nachricht entziffern oder etwas aus dem Tresor holen.

Die asymmetrische Verschlüsselung beruht auf mathematischen Verfahren, die in einer Richtung einfach aber in der anderen Richtung schwierig durchzuführen sind. Multiplizieren ist so ein Beispiel:

Jeder kann einfach zwei Zahlen multiplizieren, zum Beispiel:
3 121 163 * 4 811 953 = 15 018 889 661 339
Zahlen in Faktoren zu zerlegen, ist dagegen sehr mühselig: Hat man erst einmal das Produkt, ist es sehr schwierig herauszufinden, aus welchen Faktoren dieses

ursprünglich gebildet wurde. Versuchen Sie doch einmal (wenn Sie viel, viel Zeit haben) herauszufinden, aus welchen Faktoren die Zahl 11 099 399 206 043 besteht.

Das Problem mit dem Schlüsselaustausch ist daher elegant gelöst: Der öffentliche Teil kann jedem zugänglich gemacht werden, ohne dass die Sicherheit darunter leiden würde. Man benötigt ja immer noch den geheimen Schlüssel. Ein weiterer Vorteil des Verfahrens ist, dass sehr viel weniger Schlüssel benötigt werden als beim symmetrischen Verfahren. Denn jeder benötigt ja nur ein Schlüsselpaar.

Aber auch asymmetrische Verschlüsselungsverfahren haben Schattenseiten:

- Erstens sind asymmetrische Verfahren, im Vergleich zu symmetrischen Verfahren, sehr rechenaufwändig. Um kurze Nachrichten zu verschlüsseln, benötigt der Computer viel Zeit. Deshalb bedient man sich eines Tricks: Mit dem langsamen, asymmetrischen Verfahren werden nur die Schlüssel für ein schnelles symmetrisches Verfahren sicher und unkompliziert ausgetauscht. Die weitere Kommunikation erfolgt dann über die schnellere symmetrische Verschlüsselung. Weil asymmetrische Verfahren dafür genutzt werden, die Schlüssel eines symmetrischen Verfahrens zu verschlüsseln, nennt man es hybride - also kombinierte - Verschlüsselung.

- Zweitens kann keiner so leicht rauskriegen, ob der verwendete Public Key auch wirklich demjenigen gehört, dem man die verschlüsselte Nachricht schicken will. Im Internet ist es leicht sich für jemanden anderen auszugeben und es könnte jemand fälschlicherweise behaupten, er wäre der berechtigte Empfänger und Ihnen seinen Public Key andrehen wollen. Er könnte dann die vertrauliche Botschaft lesen. Würde er sie danach, vielleicht auch noch gefälscht, an den richtigen Empfänger weiterleiten, bliebe das ganze wahrscheinlich auch noch unbemerkt.

Diese Problematik lässt sich mithilfe einer Public Key Infrastructure (PKI) verhindern.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird zur Verschlüsselung und Entschlüsselung der gleiche Schlüssel verwendet. Dabei gibt es zwei Methoden: Blockchiffre und Stromchiffre.
Die **Blockchiffre** verschlüsseln und entschlüsseln mit einem Schritt mehrere Zeichen (=1 Block). Die **Stromchiffre** hingegen ver- und entschlüsseln Zeichenweise.

Der große **Nachteil** symmetrischer Verfahren liegt in der Nutzung ein und desselben Schlüssels zur Ver- und Entschlüsselung. Wenn ein Angreifer den Schlüssel „in die Hände bekommt“, so kann er einfach an Information gelangen und Fehlinformationen durch Veränderung der Originalnachricht verbreiten. Ein weiteres typisches Problem beim Einsatz von symmetrischen Verfahren ist, wie der Schlüssel erstmals über unsichere Kanäle übertragen werden kann. Üblicherweise kommen hierzu dann asymmetrische Kryptosysteme zum Einsatz, basierend auf dem Diffie-Hellman-Algorithmus.

Ein Beispiel für die symmetrische Verschlüsselung kommt aus der Geschichte: der so genannte **Cäsar-Chiffre**. Dieser funktioniert folgendermaßen:
Die Buchstaben des Alphabets werden durch einen um n - Stellen weiter hinten liegenden Buchstaben ersetzt. (n liegt zwischen 1 und 25, in der Tabelle ist der historische Fall mit n=3 dargestellt. Die Verschlüsselung ist sehr einfach. Die Entschlüsselung aber auch, da die Häufigkeit sich nicht ändert. Gleiche Buchstaben werden gleich chiffriert:
Originalsatz: HEUTE SCHEINT DIE SONNE.
Verschlüsselter Satz: KHXWH VFKHLQW GLH VRQQH, für n=3.

Moderne symmetrische Verschlüsselungsverfahren arbeiten ähnlich. Beispiele für moderne Verschlüsselungsverfahren sind:

Algorithmus	Methode	Bemerkung
AES (Advanced Encryption Standard)	Blockchiffre	US-amerikanische Verschlüsselungsstandard
DES (Data Encryption Standard)	Blockchiffre	bis zum Oktober 2000 der Verschlüsselungsstandard der USA
Triple-DES	Blockchiffre	Weiterentwicklung von DES
IDEA (International Data Encryption Algorithm)	Blockchiffre	Anwendung in PGP
Blowfish	Blockchiffre	1993 von Bruce Schneier entwickelt
Twofish	Blockchiffre	Anwendung in Windows
RC2, RC4, RC5, RC6 („Rivest Cipher“)	Stromchiffre	Anwendung in WEP

Tabelle 1: Symmetrische Verschlüsselungsverfahren

Beispiele aus der Praxis

Backup & Recovery

In diesem Kapitel werden die Themen Datensicherung (Backup) und Datenwiederherstellung (Recovery bzw. Restore) behandelt und Fragen geklärt wie beispielsweise „Wie kann ich meine persönlichen Daten sichern?“.

Arten der Datensicherung

Volldatensicherung (Complete Backup)

Bei einer Volldatensicherung werden sämtliche vorhandene Dateien auf einem externen Datenträger gespeichert. Dieses Verfahren ist eher ungeeignet für die tägliche Datensicherung, da sie sehr viel Zeit und Speicher in Anspruch nimmt.

Eine besondere Art der Volldatensicherung ist das Image-Backup, von dem sich auch das Betriebssystem einschließlich aller installierten Programme wieder zurückspielen lässt. Mit einem so genannten Image-Programm werden digitale Momentaufnahmen des Systems (bzw. einzelner Partitionen) erzeugt und auf einem Datenträger (z.B. DVD-Rohling) abgespeichert. Die Imagedatei enthält eine komplette Kopie der

gesamten Festplatte inklusive aller Daten, des Betriebssystems und der Programme. Beim Zurückspielen eines solchen Images lässt sich das Computersystem wieder in den gleichen Zustand, wie zum Zeitpunkt der Sicherung, zurückversetzen. Zur täglichen Sicherung der persönlichen Daten ist dieses Verfahren ebenfalls ungeeignet, da man bei der Änderung nur einer Datei das gesamte System abspeichern müsste. Ein neues Image Backup sollte daher nur vorgenommen werden, wenn grundlegende Veränderungen der Installation an Ihrem System vorgenommen wurden.
Die neuesten Versionen der Image-Programme (wie z.B. Norton Ghost) sind schon in der Lage inkrementelle Image-Backups zu erzeugen.

Im nachfolgenden Beispiel wird eine Volldatensicherung mit „Bordmitteln“, also Programmen, die bereits bei WindowsXP[1] mitgeliefert wurden, vorgenommen. Das Sicherungsprogramm befindet sich im Startmenü unter Start → Alle Programme → Zubehör → Systemprogramme → Sicherung.

Das Sicherungsprogramm startet im Assistentenmodus (beim ersten Mal und wenn dieser nicht deaktiviert wurde). Daraufhin wird abgefragt, ob man Daten sichern oder wiederherstellen möchte:

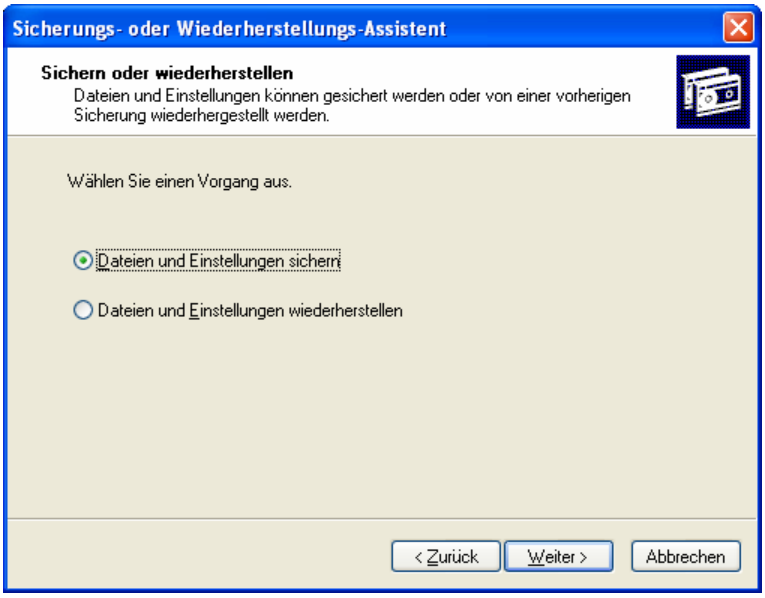


Abbildung 1: Sicherungs- oder Wiederherstellungs-Assistent Schritt 1

Im nächsten Schritt wird abgefragt, welche Daten gesichert werden sollen:

[1] Bei WindowsXP Professional ist das Sicherungsprogramm bereits installiert. Bei WindowsXP Home muss dieses erst nachinstalliert werden. Auf WindowsXP-Home-CD befindet sich im Verzeichnis VALUEADD\MSFT\NTBACKUP die Datei NTBACKUP.MSI. Mit Doppelklick auf diese Datei startet das Installationsprogramm für das Sicherungsprogramm.

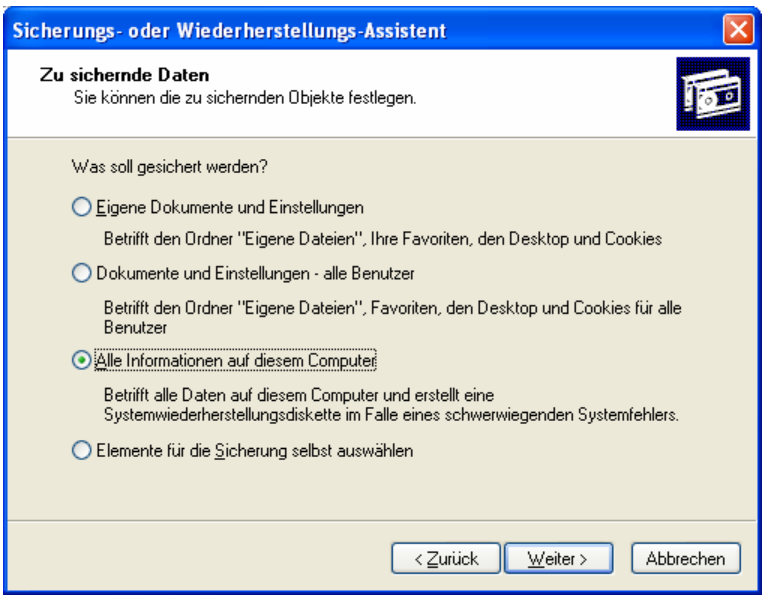


Abbildung 2: Sicherungs- oder Wiederherstellungs-Assistent Schritt 2

Dabei stehen 4 Möglichkeiten zur Auswahl. Der erste Punkt „Eigene Dokumente und Einstellungen“ sichern, speichert nur die Ordner „Eigene Datei“, die Favoriten und Cookies aus dem Internet-Explorer, sowie die Dateien und Verknüpfungen auf dem Desktop des gerade angemeldeten Benutzers. Der nächste Punkt „Dokumente und Einstellungen – alle Benutzer“ sichert die gleichen Ordner, dieses Mal für alle eingerichteten Benutzer des Computers. „Elemente für die Sicherung selbst auswählen“ bietet die Möglichkeit, einzelne Dateien und/oder Ordner in einer Sicherung zu speichern.
Der Punkt „Alle Informationen auf diesem Computer“ ist die richtige Auswahl für die Volldatensicherung. Damit soll es nun auch „Weiter >“ gehen.

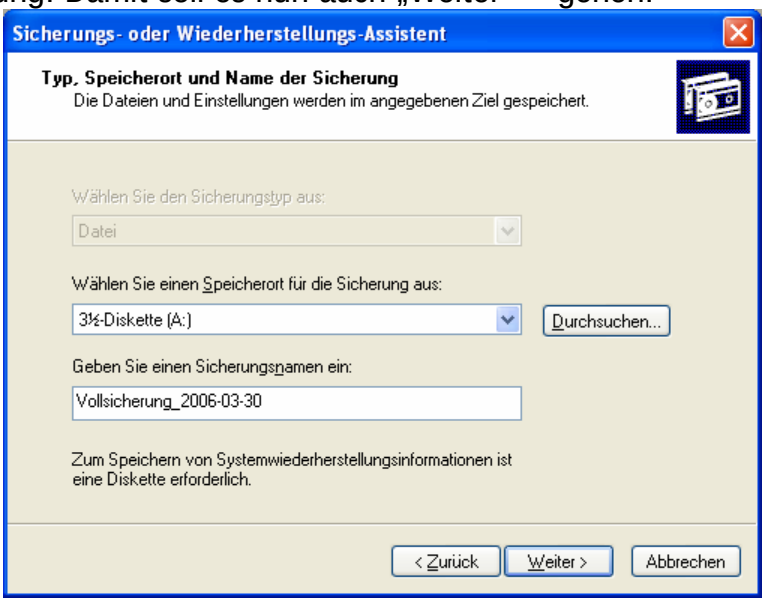


Abbildung 3: Sicherungs- oder Wiederherstellungs-Assistent Schritt 3

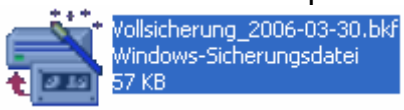
Nun besteht die Möglichkeit, die Sicherung auf 3,5Zoll-Disketten (wie hier im Beispiel), auf USB-Sticks oder in ein bestimmtes Verzeichnis (z.B. C:\Datensicherungen\) vorzunehmen. Der Name der Sicherung sollte auch eher „sprechend“ sein, da heißt es sollte aus dem Namen hervorgehen, was und wann

gesichert wurde. Ein Beispiel für einen guten sprechenden Namen wäre „Vollsicherung_2006-03-30“:
was für gesichert: Vollsicherung
wann wird gesichert: 30.03.2006 (2006-03-30; Notation rückwärts hat den Vorteil, dass bei mehreren Sicherungen gleichen Typs eine automatische Sortierung nach Datum möglich ist.)
Bevor das Sicherungsprogramm seine Arbeit aufnimmt, wird noch einmal eine Übersicht über alle Einstellungen angezeigt, die vorgenommen wurden:

Abbildung 4: Sicherungs- oder Wiederherstellungs-Assistent Schritt 4

Mit Klick auf „Fertig stellen“ beginnt das Programm mit der Sicherung aller Daten in die Datei „Vollsicherung_2006-03-30“.

Die Datei auf der Festplatte lautet nun Vollsicherung_2006-03-30.bkf:



Differenzielle Sicherung

Bei der Differenziellen Datensicherung werden alle Daten gesichert, die sich seit der letzten Volldatensicherung geändert haben. Es wird also die Differenz der veränderten Daten zum letzten Vollbackup gesichert. Dadurch wird viel Zeit und Speicherplatz gespart, da nicht mehr alle Daten erneut gesichert werden müssen. Bei der Wiederherstellung muss neben der Vollsicherung nur die aktuelle Differenzsicherung herangezogen werden.

Nachfolgend wird eine Differenzielle Sicherung mit „Bordmitteln“ gezeigt:
Starten des Sicherungsprogramms über Start → Alle Programme → Zubehör → Systemprogramme → Sicherung:

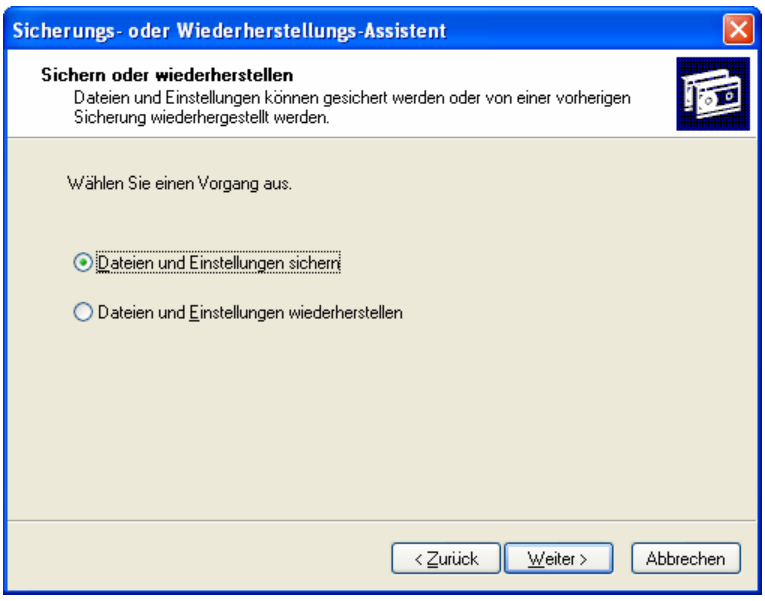


Abbildung 5: Differenzielle Datensicherung Schritt 1

In nachfolgenden Schritt soll wieder ausgewählt werden, welche Daten gesichert werden sollen. Für die Differenzielle Sicherung ungeeignet ist der Punkt „Alle Informationen auf diesem Computer“, da hier eine vollständige Datensicherung angestoßen wird. Deshalb entscheiden wir uns in diesem Beispiel für den Punkt: „Eigene Dokumente und Einstellungen“:

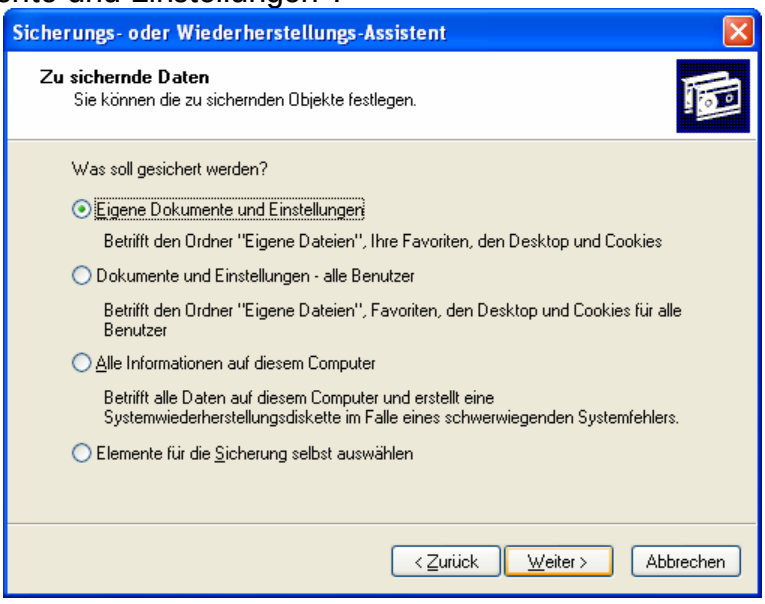


Abbildung 6: Differenzielle Datensicherung Schritt 2

Mit einem Klick auf „Weiter >“ kann ausgewählt werden, wohin die Daten gesichert werden sollen und wie der Name des Backupsatzes lautet.

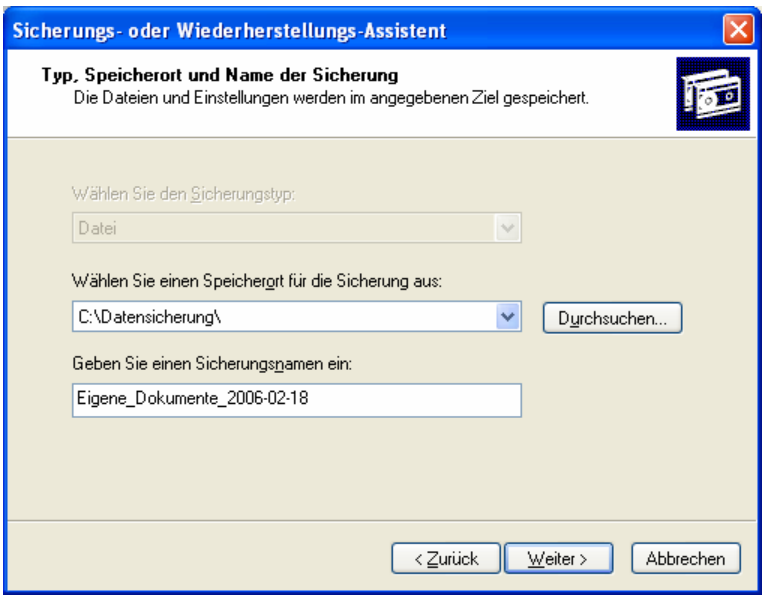


Abbildung 7: Differenzielle Datensicherung Schritt 3

Der Name der Sicherung sollte „sprechend“ sein. Als Empfehlung sollte es aus dem Namen heraus Aufschluss darüber geben, welche Daten sich in der Sicherung befinden und wann diese Sicherung gemacht wurde.
Im nächsten Schritt wird eine Zusammenfassung über die vorgenommene Konfiguration der Datensicherung angezeigt.

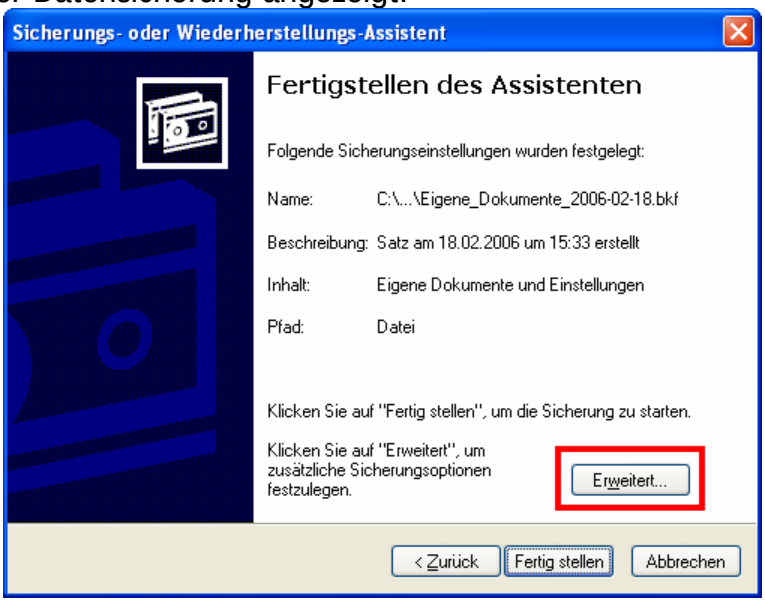


Abbildung 8: Differenzielle Datensicherung Schritt 4

Besonders wichtig ist in diesem Fenster der Button „Erweitert ...“, denn hier wird der Typ der Sicherung ausgewählt:

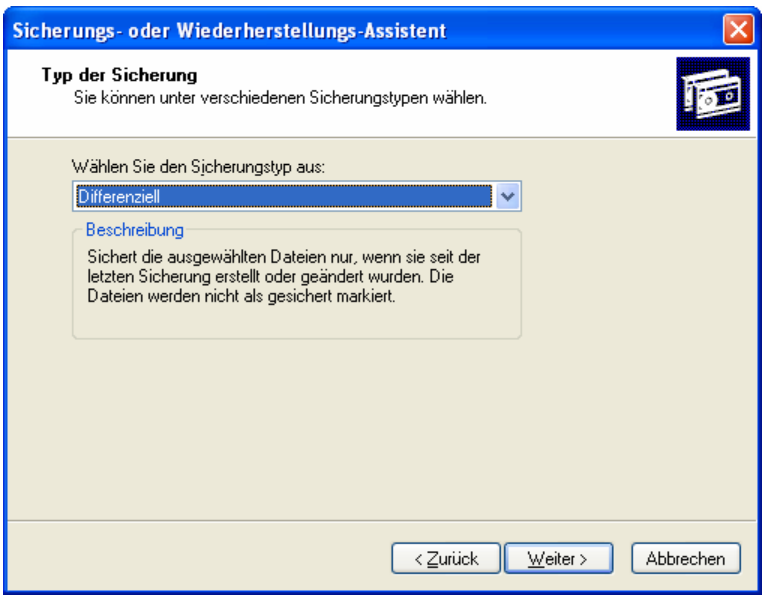


Abbildung 9: Differenzielle Datensicherung Schritt 5

Neben der Option „Differenziell“ gibt es noch 4 weitere: „Normal“, „Kopieren“, „Inkrementell“ und „Täglich“.
Die wesentlichen Unterschiede sind im Unterkapitel „Das Archivbit“ dargestellt.

Nachdem der Typ „Differenziell“ ausgewählt wurde, können nun noch zusätzliche Optionen für die Sicherung angegeben werden:

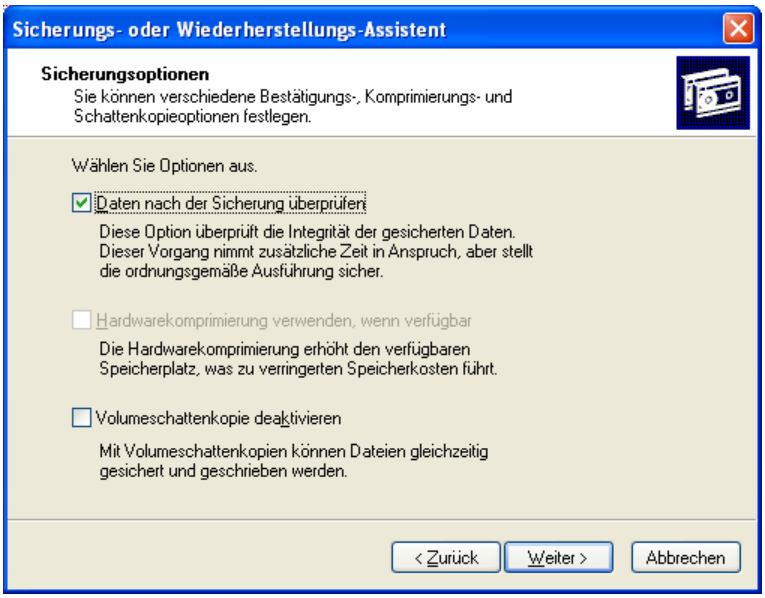


Abbildung 10: Differenzielle Datensicherung Schritt 6

Es wird empfohlen, die Option „Daten nach der Sicherung überprüfen“ zu aktivieren. Der Vorgang dauert dann etwas länger, aber man geht sicher dass die gesicherten Daten im Sicherungsarchiv lesbar sind.
Das Sicherungsprogramm bietet zudem noch im nächsten Schritt die Möglichkeit, die Datensicherung zukünftig automatisch zu bestimmten Zeiten ausführen zu lassen. Dazu muss die Option „später“ beim Schritt „Zeitpunkt der Sicherung“ ausgewählt werden und der Taskplaner aktiv sein.

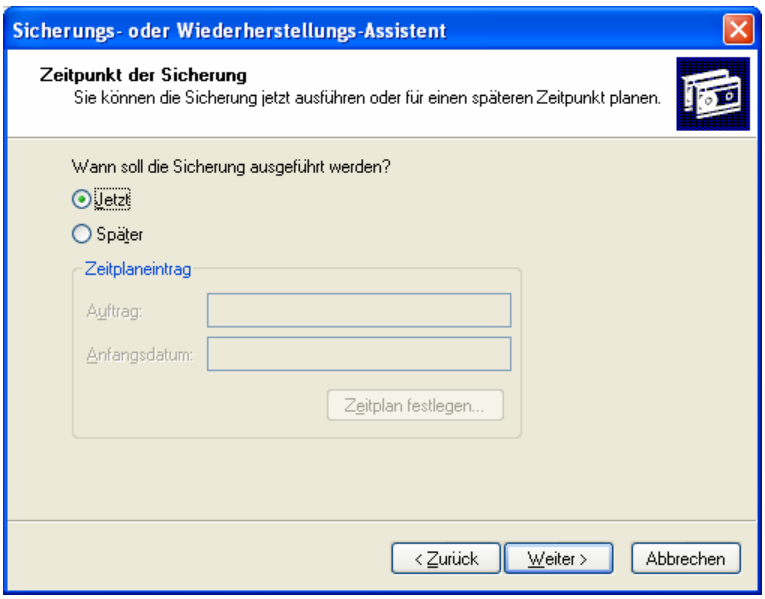


Abbildung 11: Differenzielle Datensicherung Schritt 7

Für einen einmaligen Vorgang wählt man die Option „Jetzt“ aus. Bevor nun im letzten Schritt die Sicherung gestartet wird, erhält man noch eine Zusammenfassung die man mit Klick auf „Fertig stellen“ quittiert:

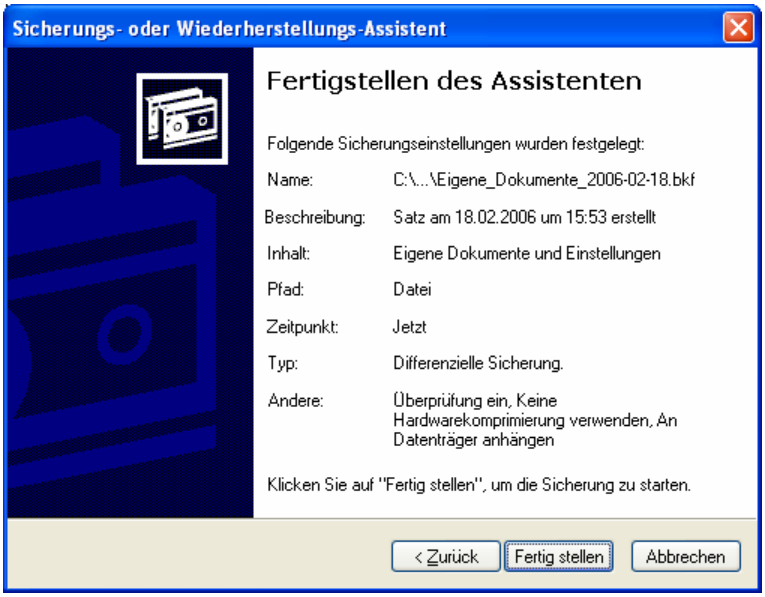


Abbildung 12: Differenzielle Datensicherung Schritt 8

Nun beginnt das Programm mit der Sicherung der ausgewählten Dateien. Dieser Vorgang dauert je nach Datenmenge wenige Sekunden bis einige Minuten. Der Fortschritt der Datensicherung wird über folgendes Fenster dargestellt:

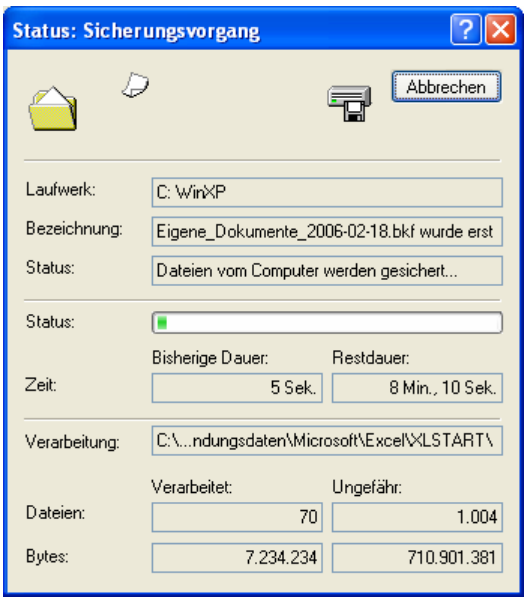


Abbildung 13: Differenzielle Datensicherung: Status Sicherungsvorgang

Inkrementelle Sicherung

Bei der inkrementellen Sicherung werden nur Daten gespeichert, die sich seit der letzten Datensicherung verändert haben. Dies kann eine Normalsicherung oder eine inkrementelle Sicherung sein.
Als Vorteil wäre der geringe Speicherplatzbedarf zu nennen. Nachteilig ist die aufwendigere Wiederherstellungsprozedur, da alle Inkremente vorhanden sein müssen.

Der Ablauf einer inkrementellen Sicherung unterscheidet sich bei der WindowsXP-Sicherung gegenüber der differenziellen Sicherung nur im Schritt 5 (siehe Abbildung 9: Differenzielle Datensicherung Schritt 5). Hier wählt man nun statt „Differenziell“ den Punkt „Inkrementell“ aus:

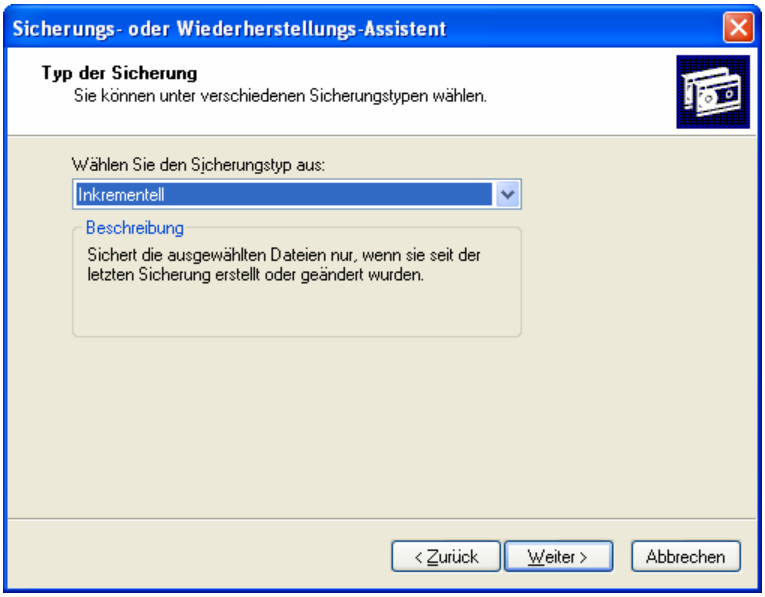


Abbildung 14: Inkrementelle Datensicherung

Das Archivbit

Das WindowsXP-Datensicherungprogramm arbeitet für manche Sicherungsarten mit dem so genannten Archivbit. Welche Arten das Archivbit nutzen, sind in der folgenden Tabelle dargestellt.

Modus	Welche Daten werden gesichert?	Archivbit
Normal	alle ausgewählten	gesetzt
Kopieren	alle ausgewählten	nicht gesetzt
Differenziell	von den ausgewählten Dateien werden alle gesichert, die sich seit dem letzten normalen Backup geändert haben	nicht gesetzt
Inkrementell	von den ausgewählten Dateien werden alle gesichert, die sich seit dem letzten Backup (normal oder inkrementell) geändert haben	gesetzt
Täglich	von den ausgewählten Dateien werden alle gesichert, die sich zum aktuellen Datum geändert haben	gesetzt

Tabelle 2: Modi des WindowsXP-Sicherungsprogramms

Jede Datei auf der Festplatte hat 4 Attribut-Bits[2], die man im Windows-Explorer sichtbar machen kann:

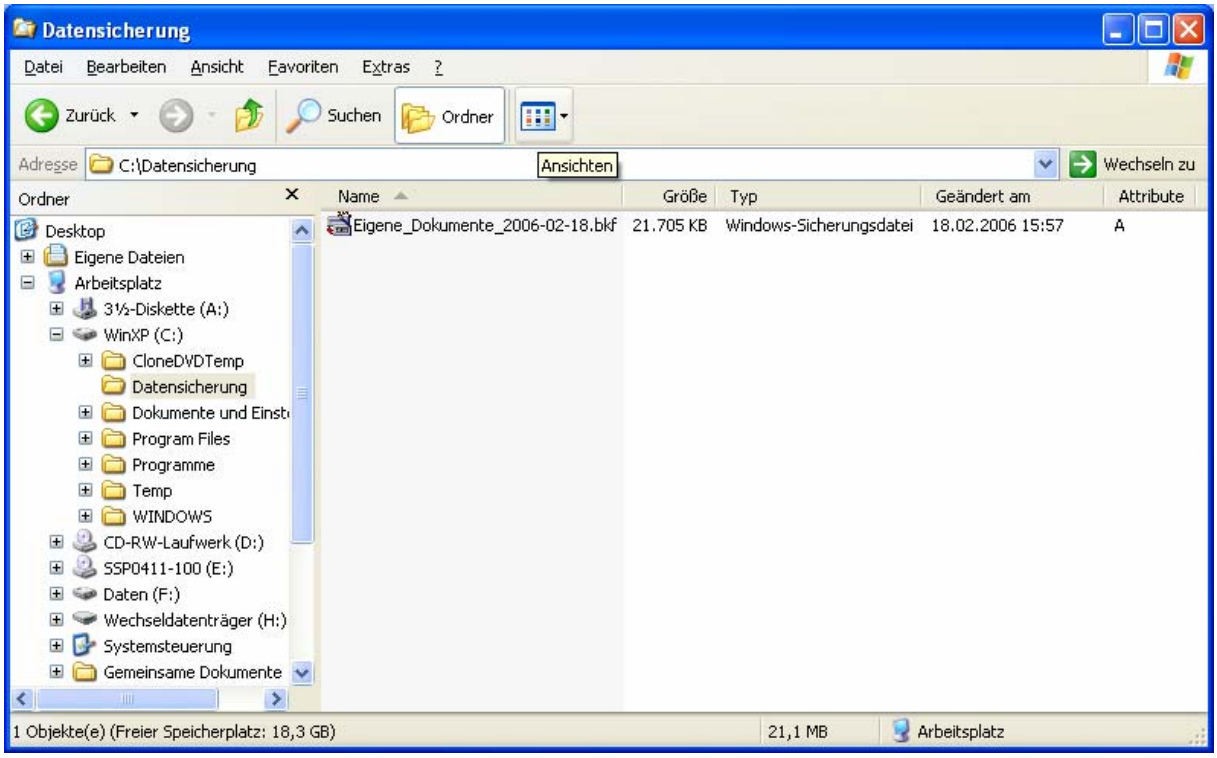


Abbildung 15: Windows-Explorer – Dateiattribute

Ruft man nun die Eigenschaften einer Datei auf, so werden die Attribute als Kontrollkästchen dargestellt:

[2] Attribute: schreibgeschützte Datei, Systemdatei, versteckte Datei und archivierte Datei

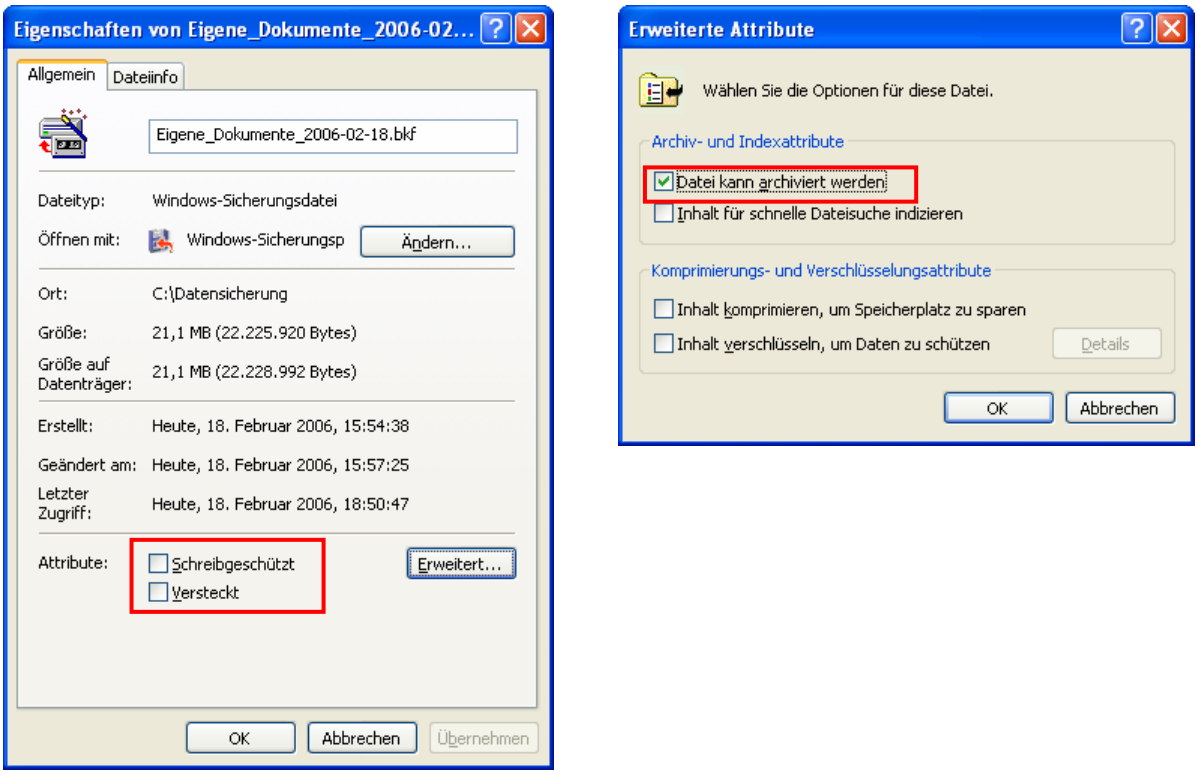


Abbildung 16: Dateiattribute in den Dateieigenschaften

Wenn das WindowsXP-Sicherungsprogramm nun eine Datei mit dem Attribut „Archiv“ versehen hat, wird diese Datei beim nächsten differenziellen Backup nicht mit gesichert, da es bereits in einem Archiv ist. Der Unterschied zum inkrementellen Backup liegt nun darin, dass das inkrementelle Backup das Archiv-Bit bei jeder zusätzlich gesicherten Datei setzt und diese als archiviert markiert. Das differenzielle Backup setzt dieses Bit nicht.

Datenrücksicherung mit Bordmitteln

Principle Of Least Privilege

Viren, Würmer und Trojaner

Im nachfolgenden Kapitel wird Schadsoftware in Form von Viren, Würmern, Trojanern, Spyware und Hoaxes genauer beleuchtet.
Der Betriebssystemhersteller Microsoft stellt auf seiner Homepage ein Programm kostenlos bereit, mit dem sich der eigene Rechner auf schadhafter Programme untersuchen lässt:
http://www.microsoft.com/germany/sicherheit/tools/malwareremove.mspx
Dieses Programm ersetzt aber keinesfalls einen Virenscanner.

Viren

Allgemeine Definition

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert.

Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware (z. B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch vom Ersteller gewünschte oder nicht gewünschte Funktionen die Computersicherheit beeinträchtigen und zählen dann zur Malware.

Der Begriff Computervirus wird auch fälschlich für Computerwürmer und Trojanische Pferde genutzt, da der Übergang inzwischen fließend und für Anwender oft nicht zu erkennen ist.

Unterschied zwischen Würmen und Viren

Computerviren und -Würmer verbreiten sich beide auf Rechnersysteme, doch basieren sie zum Teil auf vollkommen verschiedenen Konzepten und Techniken.

Ein Virus verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese ggf. so anpasst, dass das Virus auch ausgeführt wird, wenn das Wirtsprogramm gestartet wird. Zu den infizierbaren Dateien zählen normale Programmdateien, Programmbibliotheken, Skripten, Dokumente mit Makros oder anderen ausführbaren Inhalten sowie Bootsektoren (auch wenn Letztere normalerweise vom Betriebssystem nicht als Datei repräsentiert werden).

Die Verbreitung auf neue Systeme erfolgt durch versehentliches (gelegentlich auch absichtliches) Kopieren einer infizierten Wirtsdatei auf das neue System durch einen Anwender. Dabei ist es unerheblich, auf welchem Weg diese Wirtsdatei kopiert wird: Früher waren die Hauptverbreitungswege Wechselmedien wie Disketten, heute sind es Rechnernetze (z.B. via E-Mail zugesandt, von FTP-Servern, Web-Servern oder aus Tauschbörsen heruntergeladen). Es existieren auch Viren, die Dateien in freigegebenen Ordnern in LAN-Netzwerken infizieren, wenn sie entsprechende Rechte besitzen.

Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versuchen aktiv in neue Systeme einzudringen. Sie nutzen dazu Sicherheitsprobleme auf dem Zielsystem aus, wie z.B.:

- Netzwerk-Dienste, die Standardpasswörter oder gar kein Passwort benutzen
- Design- und Programmierfehler in Netzwerk-Diensten
- Design- und Programmierfehler in Anwenderprogrammen, die Netzwerkdienste benutzen (z.B. E-Mail-Clients)

Ein Wurm kann sich dann wie ein Virus in eine andere Programmdatei einfügen; meistens versucht er sich jedoch nur an einer unauffälligen Stelle im System mit

einem unauffälligen Namen zu verbergen und verändert das Zielsystem so, dass beim Systemstart der Wurm aufgerufen wird.

In der Umgangssprache werden Computerwürmer wie „I Love You“ oft fälschlicherweise als Viren bezeichnet, da der Unterschied für Anwender oft nicht ersichtlich ist.

Arten von Viren

Boot-Virus

Als "Booten" bezeichnet man das Laden des Betriebssystems. Hierbei werden u. a. Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben den Boot- oder Partitions-Sektor mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert und dann beim Start des Computers anschließend an den Virus-Code ausgeführt. Dadurch startet der Computer scheinbar wie gewohnt. Der Boot-Virus gelangt jedoch bereits vor dem Laden des Betriebssystems in den Arbeitsspeicher des Computers und verbleibt dort während der gesamten Betriebszeit. Er kann deshalb den Boot-Sektor jeder nicht schreibgeschützten Diskette infizieren, die während des Rechnerbetriebs benutzt wird, und sich auf diese Weise auf andere Computer übertragen.

Bei Computer-Netzen verwendet der File-Server in der Regel ein anderes Betriebssystem als MS-DOS. Boot-Viren können sich über diese Computer dann nicht ausbreiten. Der Boot-Versuch kann jedoch schon wichtige Systembereiche des Server-Betriebssystems zerstören.

File-Virus

Die meisten File-Viren lagern sich an Programmdateien an. Dies geschieht jedoch so, dass beim Aufruf auch hier der Virus-Code zuerst ausgeführt wird und erst anschließend das originale Programm. Dadurch läuft das Programm anschließend wie gewohnt und der Virus wird nicht so schnell entdeckt. Es sind jedoch auch primitivere, überschreibende Viren bekannt, die sich so an den Anfang des Wirts-Programms setzen, dass dies nicht mehr fehlerfrei läuft.

Wie kann man sich vor Viren schützen?

Anwender sollten **niemals unbekannte Dateien** oder Programme aus unsicherer Quelle **ausführen** und generell beim Öffnen von Dateien Vorsicht walten lassen. Das gilt insbesondere für Dateien, die per E-Mail empfangen wurden. Solche Dateien – auch eigentlich harmlose Dokumente wie Bilder oder PDF-Dokumente – können durch Sicherheitslücken in den damit verknüpften Anwendungen auf verschiedene Weise Schadprogramme aktivieren. Daher ist deren Überprüfung mit einem aktuellen Antivirenprogramm[3] zu empfehlen.

Betriebssystem und Anwendungen sollten regelmäßig aktualisiert werden und vom Hersteller bereitgestellte Service Packs und Patches/Hotfixes eingespielt werden.

[3] Kostenlose Antivirenprogramme für den Privatgebrauch sind im Anhang aufgeführt.

Microsoft bietet beispielsweise Onlineupdates (http://windowsupdate.microsoft.com) sicherheitskritische Probleme beheben. Dazu gibt es auch die Möglichkeit, die Service Packs und Hotfixes für Windows 2000 und Windows XP via „Offline-Update“[4] einzuspielen. Diese Offline-Updates sind besonders bei neuen PCs zu empfehlen, da andernfalls der PC bereits beim ersten Verbinden mit dem Internet infiziert werden könnte.

Da auf fast jedem neuen Rechner mit WindowsXP bereits der Internet-Explorer und Outlook-Express vorinstalliert sind, sind diese Programme besonders beliebte Angriffsziele für Viren. Daher empfielt es sich, diese Programme sicherer zu konfigurieren oder alternative Programme wie den Mozilla Firefox[5] oder den Opera[6]-Browser zum Surfen bzw. Mozilla Thunderbird[7] verwenden.

Würmer

Ein Computerwurm ist ein selbstständiges Computerprogramm, das sich über Computernetzwerke verbreitet, wie zum Beispiel durch Versenden infizierter E-Mails (selbstständig durch eine SMTP-Engine[8] oder durch ein E-Mail-Programm), durch IRC[9]-, Peer-To-Peer- und Instant-Messaging-Programme oder über Dateifreigaben. Die erst seit kurzem auftretenden Handywürmer verbreiten sich über Bluetooth und infizierte MMS.

Ein Wurmprogramm muss nicht unbedingt eine spezielle Schadensroutine enthalten. Da das Wurmprogramm aber sowohl auf den infizierten Systemen als auch auf den Systemen, die es zu infizieren versucht, Ressourcen zur Weiterverbreitung bindet, kann es allein dadurch gewaltige wirtschaftliche Schäden anrichten. Des Weiteren können Würmer die Belastung anderer Systeme im Netzwerk wie Mailserver, Router und Firewalls erhöhen.

Tarnung und Verbreitung

Würmer verbreiten sich derzeit meistens entweder automatisch über E-Mails oder über Netzwerke. Je mehr Möglichkeiten ein Wurm hat sich weiter zu versenden, umso erfolgreicher kann er sich verbreiten.

Verbreitung per E-Mail

Der Wurm verschickt eine Kopie von sich als E-Mail-Anhang. Der Inhalt der E-Mail zielt darauf ab, den Empfänger zu veranlassen, den Anhang zu öffnen und somit eine Infektion auszulösen. Verschiedene Techniken dienen der Tarnung des gefährlichen

[4] Offline-Updates für Windows-XP können unter folgender Webseite heruntergeladen werden: http://www.winfuture.de/UpdatePack
[5] OpenSource-Nachfolger des Netscape Navigators. Kann unter folgender Webseite heruntergeladen werden: http://www.mozilla.com/firefox/
[6] Freier Browser des Softwarehauses Opera. Kostenlos herunterzuladen unter: http://www.opera.com
[7] OpenSource-Programm zur e-Mail-Verwaltung. http://www.mozilla.com/thunderbird.
[8] SMTP steht für Simple Mail Transfer Protocol und beschreibt das Internet-Protokoll, wie e-Mails versandt werden. Eine SMTP-Engine ist also so etwas wie ein e-Mail-Server.
[9] IRC steht für Internet Relay Chat, einem textbasierten Chatsystem (ähnlich ICQ, AIM & Co.)

Anhangs. Daneben gab es auch E-Mails, die auf Sicherheitslücken im verbreiteten E-Mail-Programm Microsoft Outlook Express abzielten. Hier wurde die Schadsoftware als E-Mail-Anhang versendet und ohne Zutun des Benutzers durch Outlook Express gestartet.

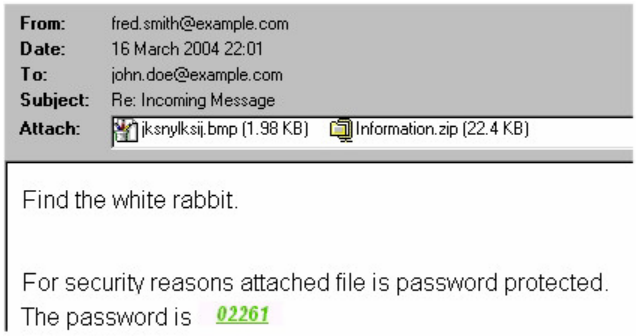


Abbildung 17: E-Mail-Wurm W32/Bagle-N

Tarnung durch doppelte Dateinamenserweiterung

Wurmprogrammdateien werden mit doppelter Dateinamenserweiterung versehen, wobei darauf gebaut wird, dass beim Empfänger die Anzeige der Dateinamenerweiterung ausgeblendet wird (Windows-Standardeinstellung). So wird beispielsweise das ausführbare Wurmprogramm „music.mp3.exe“ unter Windows nur als „music.mp3“ angezeigt und erscheint dem Opfer somit als harmlose Musikdatei. Das Öffnen dieser Datei verursacht allerdings nicht das erwartete Abspielen, sondern die unkontrollierte Ausführung des Schadprogramms.

Dateiarten, deren Ausführbarkeit dem Opfer nicht bewusst ist

Die Ausführbarkeit von „.exe“-Dateien unter Windows ist vielen Anwendern bekannt. Es gibt aber einige Dateiarten, bei denen dies nicht so gut bekannt ist. Wurm-Programmierer spekulieren deshalb darauf, dass diese Dateien nicht mit derselben Vorsicht wie „.exe“-Dateien behandelt und dadurch leichtfertig zur Ausführung gebracht werden.

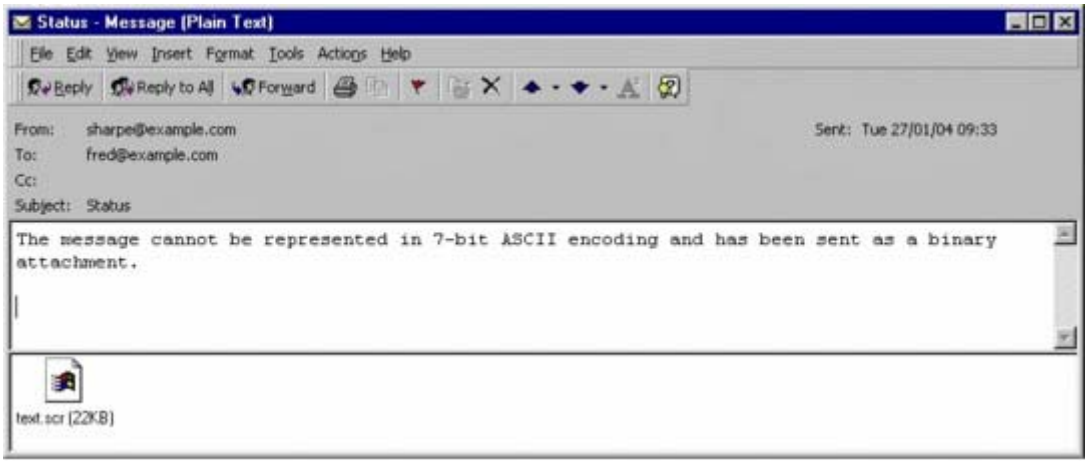


Abbildung 18: MyDoom/A als Bildschirmschoner (text.scr) getarnt

Codierung in für Antivirenprogramme unzugängliche Formate

Oft werden Würmer in ZIP-Archive[10] verpackt, um es Virenscannern zu erschweren, den Wurm zu entdecken. Zum Teil sind diese ZIP-Archive mit einem Passwort verschlüsselt, das sich im E-Mail-Text befindet. Dadurch wird es Virenscannern nahezu unmöglich gemacht, den Inhalt des Anhangs zu analysieren.

Automatisches Ausführen

Die Verbreitung der meisten Würmer ist davon abhängig, den Anwender zu Aktionen zu veranlassen, über deren Konsequenzen er sich nicht im Klaren ist. Im Allgemeinen ist dies das Öffnen der ihm zugesandten Schadsoftware. Allerdings gibt es auch Würmer, welche nicht von der Mitwirkung des Opfers abhängig sind. Sie nutzen Techniken, die ihre Aktivierung auf dem Rechner des Opfers automatisch veranlassen. Da dies grundsätzlich nicht möglich sein sollte, fällt dies unter die Kategorie „Ausnutzen von Sicherheitslücken“.

Der Wurm MS Blaster (siehe Abbildung 19: Wurm W32/Blaster-A) nutzt einen Remote-Exploit in der RPC/DCOM-Schnittstelle von Windows 2000 und XP. Das bedeutet, er nutzt eine Sicherheitslücke aus (engl. „to exploit“), um Rechner über Netzwerke zu infizieren. Nach einer Infektion beginnt er, wahllos Netze (also, z. B. das Internet) nach weiteren Rechnern mit dieser Sicherheitslücke abzusuchen, um sie unverzüglich ebenfalls zu infizieren (siehe Geschichte).

Abbildung 19: Wurm W32/Blaster-A

Wie kann man sich vor Würmern schützen?

Virenscanner

Ein Virenscanner kann im Einzelfall Infektionen verhindern, wenn vor dem Ausführen einer Datei, die einen Wurm enthält, der Virenscanner die Datei prüft, den Wurm erkennt und zugleich das Ausführen verhindert oder schon im Vorfeld bei Routine-Scans diese Datei entdeckt und der Anwender darauf aufmerksam gemacht wird.
Der Virenscanner muss – um erfolgreich arbeiten zu können – ständig aktuell gehalten werden.
Die Bereinigung eines infizierten Systems ist durch einen Virenscanner nicht zuverlässig möglich. Hersteller von Virenscannern empfehlen das Neuaufsetzen des infizierten Systems

[10] ZIP-Archive enthalten komprimierte Dateien. Andere Formate sind beispielsweise RAR-Archive (www.rarlabs.com), CAB-Archive (Microsoft Cabinet Files) oder ARJ-Archive.

Personal-Firewalls

Es kann hilfreich sein, eine Personal-Firewall-Software zu verwenden bzw. zu aktivieren. Diese kann, wenn sie richtig konfiguriert ist, Anfragen über das Netzwerk an laufende Anwendungen ausfiltern und somit das Ausnutzen von auch noch unbekannten Sicherheitslücken verhindern. Sinnvoll ist diese Maßnahme vor allem, wenn es nicht möglich ist, die Server-Anwendung zu beenden oder so zu konfigurieren, dass Anfragen nicht mehr angenommen werden oder aber wenn die Gefahr besteht, dass eine Server-Anwendung ungewollt gestartet wird. Allerdings können diese Personal-Firewalls selbst Sicherheitslücken enthalten, durch die Angreifer in ein System eindringen können.

Einschränkung der Benutzerrechte

Ausgereifte Betriebssysteme (Mac OS, Linux, Windows ab Version NT) bieten von Hause aus Sicherheitsmechanismen, welche eine Infektion deutlich erschweren bzw. unmöglich machen können. Trotzdem arbeiten beispielsweise viele Windows-Nutzer stets mit Administratorrechten. In diesem Betriebszustand sind viele Sicherheitsschranken des Betriebssystems außer Kraft. Ein versehentlich oder automatisch gestartetes Wurmprogramm (das gleiche gilt für Viren) kann sich ungehindert die Kontrolle über viele Systemfunktionen aneignen. Sinnvoller ist es, sich **zwei Benutzerkonten** einzurichten:

- eines für die routinemäßige Arbeit mit stark eingeschränkten Benutzerrechten, insbesondere eingeschränkten Rechten zur Softwareinstallation;
- das andere mit Administratorrechten allein für Installations- und Konfigurationsarbeiten.

Leider funktionieren diverse Programme unter Windows nicht oder nur unzuverlässig mit eingeschränkten Benutzerrechten. Für alle Betriebssysteme gilt aber, dass das Arbeiten mit eingeschränkten Benutzerrechten Computerwürmer nicht in jedem Fall verhindert. Grund dafür ist, dass jeder Benutzer zum Beispiel E-Mails verschicken kann.

Schaden

Der finanzielle Schaden, den Computerwürmer anrichten können, ist viel höher als jener bei Computerviren. Grund dafür ist der enorme Verbrauch an Netzwerkressourcen. Dieser Verbrauch kann zu einem Ausfall von Servern wegen Überlastung führen. Wenn ein Server ausfällt, führt das in Betrieben zu einem Arbeitsausfall. Anfang Mai 2004 erlitt eine Anzeigetafel des Flughafen Wien-Schwechat durch den Wurm „Sasser“ kurzfristig einen Totalausfall. Auswirkungen hatte dies aber nur auf das interne Informationssystem und konnte durch einen Neustart des betroffenen Computers behoben werden. Es entstanden keine Schäden, nicht einmal eine Verspätung. SQL Slammer wiederum belastete stellenweise die Internet-Infrastruktur derart, dass vielerorts die Verbindungen komplett zusammenbrachen.

Einen weiteren wirtschaftlichen Schaden können in Zukunft Handywürmer nach sich ziehen, die sich über MMS verbreiten. Wenn ein solcher Wurm dutzende kostenpflichtige MMS verschickt, ist mit einem hohen finanziellen Verlust zu rechnen.

Weitere finanzielle Schäden können durch so genannte Distributed-Denial-of-Service-Attacken entstehen. Wie am Beispiel W32.Blaster ersichtlich ist, können dadurch sogar große Betriebe wie SCO oder Microsoft in Bedrängnis gebracht werden.

Trojaner

Allgemeine Definition

Als Trojanisches Pferd bezeichnet man ein Programm, welches als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine ganz andere Funktion erfüllt.

Umgangssprachlich werden Trojanische Pferde auch Trojaner (engl. Trojan) genannt. Falsch ist dieses deshalb, weil die Trojaner eigentlich die Opfer des Trojanischen Pferdes der Mythologie geworden sind, dessen Urheber waren hingegen die Griechen. Allerdings ist der Ausdruck „Trojaner“ mittlerweile derart verbreitet, dass er weitgehend akzeptiert ist.

Schaden

Auf einem PC, auf dem ein trojanisches Pferd ausgeführt wurde, können durch eine eventuell installierte Schadroutine alle Funktionen ausgeführt werden, die der Status des angemeldeten Benutzers zulässt. Da zahlreiche Nutzer aus Bequemlichkeit oder aufgrund fehlender Kenntnis der Risiken dauerhaft mit Administratorrechten arbeiten, ist das Spektrum an Manipulationsmöglichkeiten durch die Schadroutine oder durch einen beliebigen Angreifer über das Netzwerk mittels einer Hintertür (Backdoor) unbegrenzt. Die Schadroutine kann demnach in der Regel selbstständig oder ferngesteuert alle Aktionen unentdeckt ausführen, die auch der Benutzer des infizierten Computers willentlich ausführen könnte.

Im Folgenden sind beispielhaft einige gängige Schadfunktionen aufgelistet, um einen Einblick in die Möglichkeiten der Manipulationen an infizierten Rechnern zu geben:

- Unerwünschte Werbung aus dem Internet einblenden oder den Anwender ungewollt auf bestimmte Webseiten umleiten.
- Überwachung des Datenverkehrs oder aller Benutzeraktivitäten
- Ausspähen von sensiblen Daten (Passwörter, Kreditkartennummern, Kontonummern und Ähnliches)
- Fernsteuerung von Unbekannten, u. a. für kriminelle Zwecke, z. B. zum Versenden von Werbe-E-Mails oder Durchführung von DDoS-Attacken.
- Installation von illegalen Dialer-Programmen (heimliche Einwahl auf Telefon-Mehrwertrufnummern), was dem Opfer finanziellen Schaden zufügt.

Allerdings muss ein Trojaner nicht zwangläufig über eine Schadroutine verfügen. Sendet beispielsweise das Programm ohne Wissen des Anwenders unsensible statistische Daten an den Programmierer und lässt der offensichtliche Teil des Programms keinen Rückschluss auf die versteckte Funktionalität zu, so erfüllt das Programm alle Bedingungen, um auch als Trojaner klassifiziert zu werden, obgleich

es keinen Schaden anrichtet. Zudem kann die geheime Funktion zu einer Schadroutine werden, ohne dass der Entwickler des Programms das beabsichtigt hat. Bezogen auf dieses Beispiel wäre das der Fall, wenn die Routine eine Internetverbindung aufbaut und dabei kosten verursacht oder die Netzwerkanbindung dadurch spürbar verlangsamt wird.

Wie kann man sich vor Trojanern schützen?

Aus den Charakteristika von Trojanischen Pferden ergibt sich direkt, dass es nur eine Schutzmöglichkeit vor der Infektion durch trojanische Pferde geben kann: Vermeidung der Benutzung von Programmen aus unbekannten oder unsicheren Quellen. Als besonders gefährlich einzustufen sind hierbei, wie bei jeder Malware, Anbieter von Programmen bzw. Dienstleistungen am Rande der Legalität.

Wie auch bei Computerviren schützen Antivirenprogramme in der Regel nur vor bekannten Trojanischen Pferden.

Personal Firewalls oder andere Programme zur Netzwerküberwachung bieten keinen Schutz vor der Installation eines Trojanischen Pferdes, können unter Umständen aber nach einer Infektion auf unautorisierte Netzwerkkommunikation aufmerksam machen und diese unterbinden.

Spyware

Allgemeine Informationen

Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software (das sogenannte Call Home) oder an Dritte sendet. Oft wird Spyware verwendet, um Produkte kostenlos anzubieten.

Meist dienen die Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren, um diese Daten kommerziell zu nutzen oder um gezielt Werbebanner oder Popups einzublenden, die an die Interessen des Benutzers angepasst sind. Die Firmen erhoffen sich davon eine Steigerung der Wirksamkeit dieser Werbemethoden.

Um Ärger mit Juristen zu umgehen, kennzeichnen viele Computerprogramme mit Anti-Spyware-Funktionen diese Softwarekomponenten als „möglicherweise unerwünschte Software“ (PUS, potentially unwanted software).

Spyware wird im Gegensatz zu Viren auch von Unternehmen programmiert. Mitunter werden ganze Entwicklungsabteilungen damit beauftragt. Diese Spyware hat demzufolge oft auch ein sehr hohes technisches Niveau. Beispielsweise schützt sich Spyware gegen Löschung dadurch, dass mehrere Prozesse gleichzeitig laufen, die bei Beendigung gleich wieder einen neuen aufmachen und sich selbst kopieren. Auf der Festplatte entziehen sie beispielsweise dem Administrator die Schreib- und damit die Löschberechtigung usw.

Ein weiteres Problem entsteht dadurch, dass Spyware zusätzliche Sicherheitslöcher in einem System erzeugen kann, gegen die es dann auch keine Software-Updates gibt.

Durch diese Verfahren wird es selbst einem technisch versierten User extrem schwer gemacht, sich dieser Spyware zu entledigen. Seit längerem haben sich Antivirensoftware-Hersteller des Problems angenommen und auch Lösungen gegen Spyware entwickelt.

Wie kann man sich vor Spyware schützen?

Schutz vor Spyware kann kein System richtig bieten, da Spyware teilweise in renomierten Software-Produkten vorhanden ist. Neben dem aktuell zu haltenden Virenscanner helfen Tools wie „AdAware“[11] oder „Spybot Seek & Destroy“[12]. Microsoft verfolgt mit seinem Programm „One Care“ bzw. „AntiSpy“ das Ziel, einen permanenten Schutz gegen Spyware zu etablieren. Noch befindet sich das Programm in der Testphase und kann da kostenlos genutzt werden. Später wird das Tool kostenpflichtig.

Hoaxes

Seit Jahren kursieren Warnungen vor (angeblichen) Viren, die sich per E-Mail verbreiten sollen. Diese "Warnungen" werden meist von gutgläubigen Menschen verbreitet, die diese per E-Mail von ihresgleichen erhalten haben. Sie zeigen dabei oft sogar ein Engagement, das man sich sonst nur wünschen könnte, im Glauben, sie täten den Adressaten einen Gefallen, in dem sie sie vor gefährlichen Viren warnen. Die Empfänger werden aufgefordert, E-Mails, die im Betreff (subject) einen der weiter unten genannten Begriffe enthalten, nicht zu lesen sondern sofort zu löschen. Andernfalls würde ein Virus furchtbare Dinge mit dem Rechner des Empfängers anrichten. In gleicher Weise (als Kettenbriefe) werden auch andere Falschmeldungen unterschiedlichster Art verbreitet.
Fakt ist, dass alle diese Warnungen keinen ernstzunehmenden Hintergrund haben (was die Gefährlichkeit der vermeintlichen Viren angeht). Es handelt sich wohl mehr um ein soziologisches Phänomen. Es gibt die E-Mails, vor denen gewarnt wird, meist gar nicht. Diese Warnungen werden Hoaxes genannt (engl. hoax, altengl. hocus: Scherz, Falschmeldung). Vielmehr stellen diese "Warnungen" die eigentlichen Viren dar, denn sie richten erheblichen Schaden an, in dem sie Menschen verunsichern und Arbeitszeit binden. Außerdem belasten sie durch ihre nicht geringe Zahl das Internet durch nutzlosen Datenverkehr. Generell werden nie echte Virus-Warnungen auf diese Weise in die weite Welt geschickt. Sehr wohl können aber Viren in Dateianhängen (Attachments) von E-Mails enthalten sein.

Eine Liste aktueller und historischer Hoaxes finden sich auf der Homepage der TU Berlin unter folgender Adresse: http://www.tu-berlin.de/www/software/hoax.shtml

[11] AdAware von Lavasoft, Programm zum Entfernen von Spyware (auch als kostenlose Version erhältlich): http://www.lavasoftusa.com/software/adaware/
[12] SpyBot Seek&Destroy ist ein Programm zum Entfernen von Spyware: http://www.safer-networking.org/de/index.html

Passwörter

Was ist ein Passwort?

Ein Kennwort oder auch Passwort ist ein allgemeines Mittel zur Authentifizierung eines Benutzers (nicht ausschließlich ein Mensch) innerhalb eines Systems, der sich durch eine eindeutige Information (das Kennwort) dem System gegenüber ausweist. Die Authentizität des Benutzers bleibt daher nur gewahrt, wenn er das Passwort geheim hält.

Einsatz von Kennwörtern

Häufiger Einsatz von Kennwörtern findet in der Computerwelt in Verbindung mit einem Benutzernamen statt, z.B. bei TWT PRIMA. Hier ist das Kennwort eine beliebige, vom Nutzer gewählte Zeichenfolge. Einen Sonderfall stellt das so genannte Einmalpasswort dar, bei dem jedes Passwort nur einmal zur Authentisierung benutzt wird und dann ungültig wird. Diesem Vorgehen wird eine besonders hohe Sicherheit zugesprochen. Es entsteht kein Schaden, wenn ein Einmalpasswort während der Benutzung ausgespäht wird, denn danach ist es ja ungültig. Einmalpasswörter werden zum Beispiel für das PIN[13]/TAN[14]-Verfahren beim Online-Banking verwendet. Kennwörter werden außerdem im Bereich der Kindersicherung verwendet, um Kindern den Zugriff auf Fernseher, Receiver oder ungeeignete Programminhalte zu verwehren.

Wann ist ein Kennwort ein sicheres Kennwort?

Moderne Verschlüsselungsverfahren sind extrem stark und können in der Praxis selbst mit größtem Aufwand nicht geknackt werden. Der Schwachpunkt ist in der Regel das vom Benutzer verwendete Passwort. Dieses kann häufig mit einem Wörterbuchangriff gefunden werden. Damit ein Passwort nicht unsicherer ist als die eigentliche Verschlüsselung (hier ein 128-Bit-Schlüssel angenommen), muss dieses aus mindestens sieben zufälligen Wörtern bestehen.
Weil es sich dabei nicht mehr um ein einzelnes Wort handelt, spricht man auch von einer Passphrase. Eine relativ gute Passphrase wäre zum Beispiel: „Ich kaufe mir heute einen Kaffee für 1€ beim Bäcker.“ Es ist verhältnismäßig **leicht zu merken**, **ausreichend lang** und lässt **keine Rückschlüsse auf den Benutzer** zu.
Ungeeignet sind beispielsweise Filmzitiate (z.B. „Schau mir in die Augen, Kleines.“) oder berühmte Aussprüche, das Geburtsdatum der Großmutter oder der Name des Haustiers.

Die Sicherheit eines Kennwortes hängt vor allem davon ab, dass dieses **geheim** bleibt. Andere Faktoren zum Schutz des Kennwortes sind z.B.:

- **Häufigkeit der Verwendung**: Die größte Sicherheit ist bei einmaliger Verwendung gegeben. Jeder wiederholte Einsatz des Kennwortes erhöht die Gefahr, bei unverschlüsseltem Transfer oder Spionage-Maßnahmen (wie z.B. durch Keylogging oder Phishing) das Kennwort zu verraten.

[13] PIN steht für Persönliche Identifikationsnummer (engl. Personal Identification Number)
[14] TAN steht für Transaktionsnummer (engl. Transactionnumber)

- Die **Übertragung des Kennwortes** vom Benutzer zum System sollte sicher sein, z.B. durch Verwendung von verschlüsselten Kanälen zur Übertragung (z.B. SSL[15]). Dadurch wird es bei sicherer Implementierung und ausreichender Stärke der Verschlüsselung für den Angreifer nahezu unmöglich, das Kennwort in Erfahrung zu bringen. Die Rechenkapazität heutiger Rechner reicht nicht ausreicht, um SSL-Verschlüsselungen zu knacken.
- Viele Kennwörter können von Angreifern leicht erraten werden. Da die meisten Kennwörter von menschlichen Benutzern eingegeben werden (im Gegensatz zur Erzeugung durch Zufallsgeneratoren) und vor allem leicht einprägsam sein müssen, kommen häufig einfach zu ratende Kennwörter zum Einsatz, wie z.B. Name der Frau, des Freundes oder Haustieres, sowie Geburtstage oder Adressen.
- Die **Aufbewahrung des Kennwortes** auf der Seite des Authentisierers[16] sollte auch verschlüsselt erfolgen, die Kontrolle kann dank kryptographischer Verfahren (sogenannter Hash-Funktionen) trotzdem problemlos erfolgen.
- Das Kennwort sollte **möglichst lang** sein. Das System sollte einen möglichst großen Zeichensatz[17] verwenden, mit dem das Kennwort gebildet wird.
- Zudem sollte das System nach einer bestimmten Zahl von fehlerhaften Eingaben keine neuen Eingaben akzeptieren, bis eine bestimmte Zeit vergangen ist bzw. das System manuell wieder freigeschaltet wurde.

Angriffe auf Passwörter

Angriffe auf Kennwörter finden immer wieder statt. Die populärsten Verfahren dazu sind der Brute-Force-Angriff und der Wörterbuchangriff.

Brute-Force-Angriff

Brute-Force bedeutet auf Deutsch etwa: "Methode der rohen Gewalt". Bei einer Brute-Force-Attacke in der Kryptoanalyse werden alle möglichen Schlüssel nacheinander durchprobiert. Deshalb spricht man auch von vollständiger Schlüsselsuche. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt, dies ist aber bei üblicherweise (pseudo-)zufällig generierten Schlüsseln wenig hilfreich. Die Schlüssellänge spielt ebenfalls eine Rolle, da im Schnitt mindestens die Hälfte aller Möglichkeiten probiert werden muss, bevor der Schlüssel gefunden wird. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ schwachen Passwortes ausgegangen werden kann.

Ein Angriff auf das Verschlüsselungsverfahren selbst ist bei modernen Algorithmen unter Verwendung eines entsprechend komplexen Schlüssels in der Praxis aussichtslos. Es würde selbst unter Einsatz von mehreren Millionen Hochleistungscomputern Jahrtausende dauern, um nur einen nennenswerten Bruchteil der Möglichkeiten durchzuprobieren.

[15] SSL steht für „Secure Sockets Layer“ und beschreibt eine verschlüsselte Datenübertragung für das Internet (Datenübertragungsprotokoll).
[16] Der Authentisierer ist das Programm, welches die Passwörter auf der Gegenseite prüft.
[17] Mit großem Zeichensatz sind Zeichen aus dem Bereich der Zahlen, Buchstaben und Sonderzeichen gemeint. Zahlen bieten beispielsweise 10 Möglichkeiten, Großbuchstaben 26 und Kleinbuchstaben 26. Durch Verwendung von Elementen aus allen 3 Bereichen erhöht man die Komplexität der Kennwörter.

Daher gilt eine Brute-Force-Attacke in der Praxis immer dem konkreten Passwort. Diese allerdings ist auch in der Praxis sehr häufig erfolgreich, da die meisten Benutzer kurze Passworte verwenden. Schon auf einem handelsüblichen Computer können mehrere hunderttausend Passworte pro Sekunde ausprobiert werden.

Hier ist eine Übersicht zur Abhängigkeit zwischen Schlüssellänge und Zeit zum Entschlüsseln. Die Anzahl der Kombinationen, die pro Sekunde getestet werden, liegt für heutige „normale“ Rechner (Athlon XP 2800+) bei ca. 3 Millionen. Diese Anzahl ist Grundlage für die folgende Tabelle:

		maximale Zeit zum Entschlüsseln		
Länge	Mögl.Kombinationen	in Sekunden	in Tagen	in Jahren
1	62,00	0,00		
2	3844,00	0,00		
3	238328,00	0,08		
4	14776336,00	4,93		
5	916132832,00	305,38		
6	56800235584,00	18.933,41		
7	3521614606208,00	1.173.871,54	13,59	
8	218340105584896,00	72.780.035,19	842,36	2,31
9	13537086546263600,00	4.512.362.182,09	52.226,41	143,09
10	839299365868340000,00	279.766.455.289,45	3.238.037,68	8.871,34
11	52036560683837100000,00	17.345.520.227.945,70	200.758.335,97	550.022,84
12	3226266762397900000000,00	1.075.422.254.132.630,00	12.447.016.830,24	34.101.415,97

Wie man aus dieser Tabelle ablesen kann, erhöht sich die Anzahl der Kombinationen und die Zeit zum Entschlüsseln drastisch mit der Länge des Passworts.

Wörterbuchattacke

Als einen Wörterbuchangriff (engl.: dictionary attack) bezeichnet man die Methode der Kryptoanalyse, ein unbekanntes Passwort (oder Benutzernamen) mit Hilfe einer Passwortliste zu knacken.
Man verwendet diese Methode, wenn man davon ausgehen kann, dass das Passwort aus einer sinnvollen Zeichenkombination besteht. Dies ist, erfahrungsgemäß, meistens der Fall. Erfolg versprechend ist dieses Verfahren nur, wenn möglichst viele Passworte schnell hintereinander ausprobiert werden können.
Der aktive Wortschatz einer Sprache liegt in der Regel bei 50.000 Worten. Somit können dutzende Sprachen innerhalb weniger Sekunden überprüft werden. Ein Passwort, welches nur aus ein oder zwei Worten besteht, ist daher bei der Verschlüsselung von Texten sehr unsicher.
Durch ein spezielles Programm werden die Einträge der Passwortliste als Benutzername oder Passwort durchprobiert. Möglich ist auch das Verwenden von zwei getrennten Listen für Benutzername und Passwort. Viel häufiger ist jedoch die Verwendung einer Combo-List, einer kombinierten Liste aus Benutzername und Passwort solchen Formats: Benutzername:Passwort

Schützen kann man sich vor einer solchen Attacke am besten, in dem man „kryptische“ Passwörter verwendet bzw. Sonderzeichen in seinen Passwörtern oder Passwortsätzen verwendet.

Passwortverwaltung durch Programme

Passwordsafe

Password Safe wurde ursprünglich von dem Kryptografie-Experten Bruce Schneier entwickelt. Es handelt sich dabei um ein OpenSource[18]-Programm, welches verschiede Passwörter für verschiedene Programm und Webseiten verwaltet, mit denen ein Benutzer zu tun hat. Vorteil: Als Benutzer muss man sich nun nicht jedes einzelne Passwort merken, sondern nur das Passwort für den Passwort-Safe. Die Passwörter werden in einer sehr stark verschlüsselten Datenbank aufbewahrt. Über einen Doppelklick auf ein Element wird das Passwort in die Zwischenablagen kopiert und kann so das gewünschte Passwort im benötigten Programm einfügen.

Webseite: http://passwordsafe.sourceforge.net
Download der deutschen Version: http://passwordsafe.sourceforge.net/pwsafege.zip

Das Programm ist verfügbar für alle neueren Windows-Betriebssysteme (Windows XP, Windows 2000, Windows NT4, Windows 98, Windows 95 und Windows CE für PocketPCs) und für Linux-Betriebssysteme.

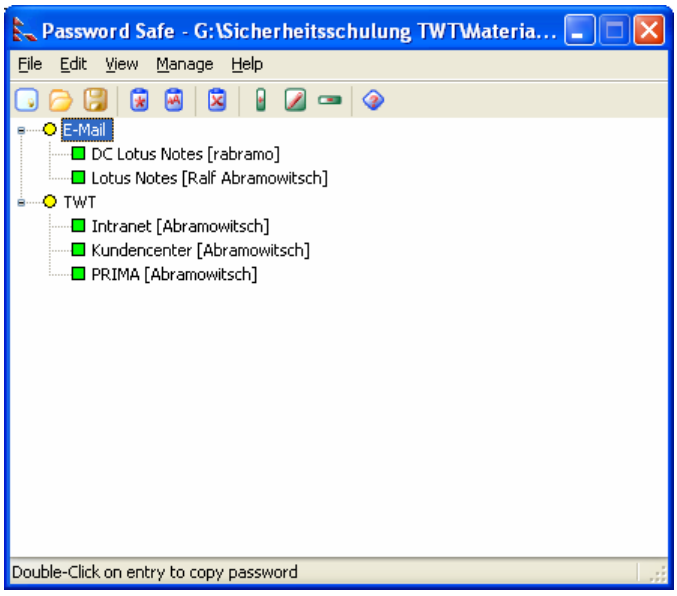


Abbildung 20: Passwort Safe

Password Safe enthält noch einen Passwort-Generator, der komplexe Kennwörter per Knopfdruck erstellt.

[18] OpenSource-Programme sind Programme, die es erlauben, einen Einblick in den Quelltext des Programms zu haben, sowie diesen Quellcode auch beliebig weiterzugeben oder zu verändern.

KeePass

KeePass Password Safe ist wie Passwort Safe ein OpenSource-Programm, mit dem man Passwörter in einer stark verschlüsselten Datenbank verwalten kann.

Webseite:
http://keepass.sourceforge.net

KeePass ist ebenfalls für alle aktuellen Windows-Betriebssysteme verfügbar.

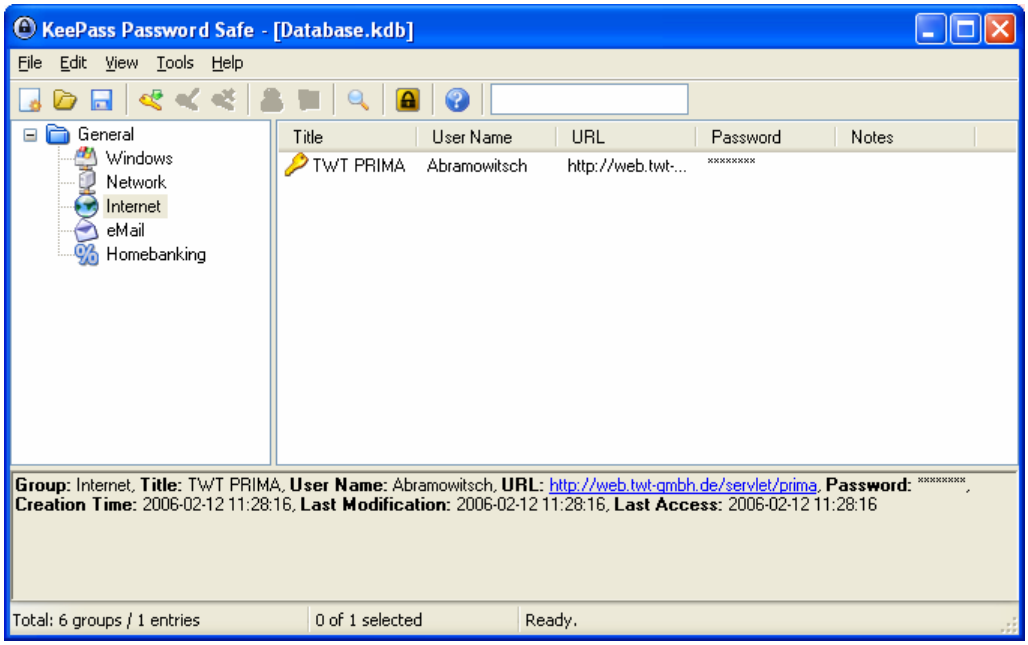
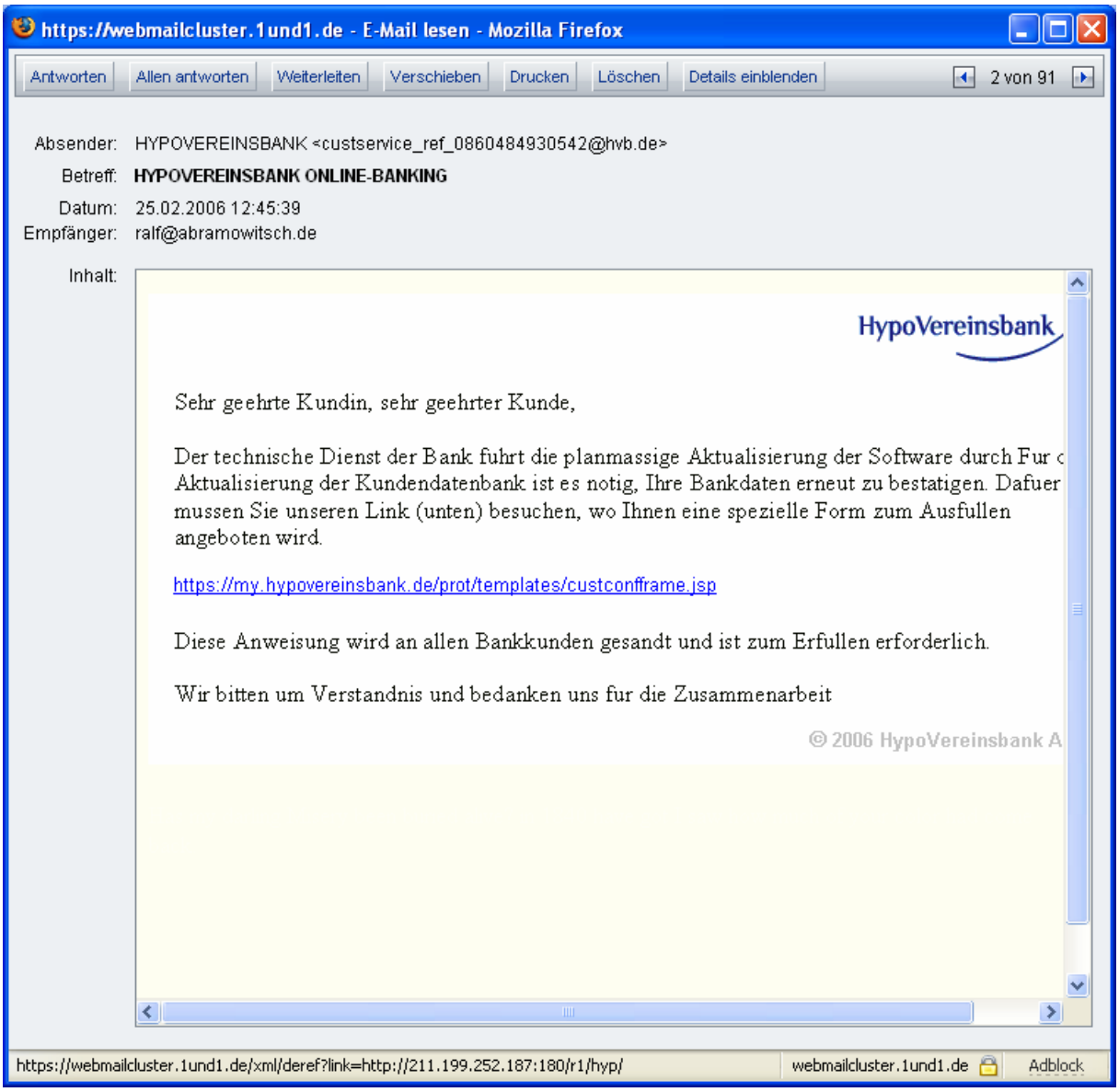


Abbildung 21: KeePass Password Safe

KeePass zeigt über eine Farbskala weiterhin an, ob das verwendete Kennwort sicher ist oder nicht. Es enthält – wie Password Safe auch – einen Passwort-Generator, der komplexe Kennwörter erzeugt.

Sicherheit im Internet

Phishing



Links

Antivirenprogramme

Kostenlose Programme

H+B EDV Antivirus: http://www.free-av.de
ClamWin Free: http://www.clamwin.com/
Bitdefender7: http://www.bitdefender.de/bd/site/products.php?p_id=24
Free Avast4 Home Edition: http://www.avast.com/eng/avast_4_home.html

Vintige AV: http://www.vintage-solutions.com/English/Antivirus/Super/index.html
Free AVG: http://free.grisoft.com/doc/1

Kostenpflichtige Programme

Norton Antivirus:
http://www.symantec.com/region/de/product/index_homecomp.html
McAfee Antivirus: http://de.mcafee.com/root/package.asp?pkgid=144
TrendMicro PcCillin: http://de.trendmicro-europe.com/index_consumer.php
Panda Antivirus: http://www.pandasoftware.com/products/activescan.htm

Firewalls

Kostenlose Programme

WindowsXP SerivicePack2 Firewall: http://windowsupdate.microsoft.com
Sygate Personal Firewall: http://www.blitzbox-download.com/spf.exe
ZoneAlarm: http://www.zonelabs.com
Kerio Personal Firewall: http://www.sunbelt-software.com/Kerio-Download.cfm
Schönherr Personal Firewall: http://www.gratis-firewall.de/download/shfw3611.exe

Kostenpflichtige Programme

Norton Internet Security:
http://www.symantec.com/region/de/product/index_homecomp.html
McAfee Personal Firewall: http://de.mcafee.com/root/package.asp?pkgid=144
ZoneAlarm Pro: http://www.zonelabs.com

Datensicherungs-Software

Kostenlose Programme

WindowsXP Sicherung (siehe Kapitel „Volldatensicherung (Complete Backup)“)
Sleepwell: http://sleepwell.cws-trummer.biz/

Kostenpflichtige Programme

Arconis TrueImage: http://www.acronis.de/homecomputing/products/trueimage/
Norton Ghost: http://www.symantec.com/region/de/product/ghost/pe_index.html
Veritas Backup Exec: http://www.backupexec.com/de/

Sicherheits-Updates für WindowsXP

Online-Updates für WindowsXP

Windows-Update-Seite: http://windowsupdate.microsoft.com

Offline-Updates für WindowsXP

Winfuture-Updatepack: http://www.winfuture.de/UpdatePack

Sicherheitschecks

Security Check: http://webscan.security-check.ch

Quellennachweise

Online-Quellen

Wikipedia – die freie Enzyklopädie
http://www.wikipedia.de

Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI)
http://www.bsi.de

TecChannel
http://www.tecchannel.de

Microsoft Deutschland
http://www.microsoft.de

Offline-Quellen

Windows-Sicherheit Das Praxisbuch
T. Weltner, K. Wilke, B. Schneider
Microsoft Press
ISBN: 3-86063-686-3

Glossar

Backup

Abbildungsverzeichnis