
Datensicherheit
Datenschutz
Urheberrechte
§§

**INHALTSVERZEICHNIS**

# 1 Einleitung

Heutzutage ist es sehr wichtig Daten vor Naturereignissen aber auch vor Viren und dergleichen zu schützen. In dieser Dokumentation lernen Sie den Unterschied zwischen Datensicherheit und Datenschutz kennen, Sie werden mit verschiedenen Virenarten bekannt gemacht und sollten nach dem lesen wissen, wie Sie sich und Ihre Daten am besten schützen.
Zusätzlich wird auch noch in das Thema Urheberrecht eingeführt, damit Sie auch wissen welche Daten Sie einfach so brauchen dürfen und welche Daten geschützt sind.
Das Dokument richtet sich nicht an Securityexperten, es soll eher Endbenutzern und Homeanwendern eine kurze Übersicht über das Thema Computersicherheit geben. Natürlich können hier nicht alle Aspekte dieses Bereiches behandelt werden. Der Anwender sollte sich auch überlegen wie er sich und seine Daten mit einfachsten Mitteln, z.B. abschliessen der Tür, Aufbewahrung der Sicherungen an einem physikalisch gesicherten Ort schützen kann.

# 2 Datensicherheit

## 2.1 Definition Datensicherheit

Unter Datensicherheit versteht man die Sicherheit, die gewährleistet wird, um Daten vor unbefugten Personen oder vor sonstigen Beeinträchtigungen (z.B. Viren) zu schützen. Um dies einhalten zu können sind Zugriffskontrollen, hochmoderne Servertechnik und Massnahmen der Datensicherung nötig. Beispiel: Bandsicherung, Sicherung der Daten gegen Umwelteinflüsse (Feuer, Hochwasser, Erdbeben etc.)

## 2.2 Unterschied Datensicherheit und Datenschutz

Die Datensicherheit befasst sich mit dem Thema: Wie können Daten sicher aufbewahrt werden gegen Umwelteinflüsse, etc. geschützt, wobei sich der Datenschutz um die Rechte der juristischen Personen (Firmen, Vereine, etc.) sowie natürlichen Personen (z.B. Sie und ich .....) vor Verletzung der Vertraulichkeit, um den Schutz der Integrität und um die Verfügbarkeit der Daten kümmert.

## 2.3 Aktuelle Bedrohungen

Es gibt drei Klassen von Bedrohungen.

- **Persönliche Motive**
- **Bereicherungsmotive**
- **Politische Motive**

**Persönliche Motive:** Meistens sind die persönlichen Motive mit Stress, Rache, Neugier oder einfach mit der technischen Herausforderung verbunden. Wenn das Arbeitsklima in einer Firma schlecht ist, können oft Verletzungen des Datenschutzes vorkommen, da jemand Rache ausüben will oder Mobbing unter den Arbeitskollegen betreibt. Natürlich spielt die menschliche Neugier etwas Neues auszuprobieren oder einfach mal selbst ein Passwort zu knacken auch eine wichtige Rolle im Bereich Datenschutz. Als Hauptbedrohung stuft man die Viren ein, sie können von praktisch jedem in ein Netzwerk geleitet werden und ein Netzwerk lahm legen.

**Bereicherungsmotive:** Unter den Bereicherungsmotiven wird z.B. Diebstahl verstanden, der meistens von Insidern (Mitarbeitern) durchgeführt wird. Es werden häufig Datenträger geklaut die mit Informationen über neue Produkte gefüllt sind und den Konkurrenzfirmen dienen können.

Datenklau wird oft ermöglicht durch zu wenig sicheren Aufbewahrungsorten der Datenträger im Firmengebäude.

**Politische Motive:** Angriffe gegen Staaten kommen im Rahmen von Hackversuchen und Virenattacken, die bösartige Folgen haben können vor. Meistens werden solche Angriffe von radikalen Gruppierungen gegen den Staat oder von Staat zu Staat gestartet.

Unter den aktiven respektive passiven Bedrohungen versteht man im Speziellen die Sichtbarkeit des Angriffs. z.B. sichtbarer Portscan oder verdeckter Portscan.
Oder Viren die sich sichtbar einschleichen und gleich etwas anrichten, oder das System erst im Laufe der Zeit angreifen und sich dann später als totale Zerstörer erweisen.
Einige Beispiele der aktiven respektive passiven Bedrohungen:

aktive: - eindringen in ein Netzwerk oder Computersystem
passive: - abhören von Verbindungen
- Umwelteinflüsse
- brand im Gebäude

## 2.4 Massnahmen gegen Bedrohungen

Prinzipiell ist Sicherheit immer teuer und schläft sich auf die „Benutzerfreundlichkeit nieder“. Jedoch kann teilweisse nur mit mässigen finanziellen Mitteln ein grundlegender Schutz erreicht werden. Es gilt das richtige Mittelmass zwischen Sicherheit und Benutzerfreundlichkeit zu finden. Je nach Branche eines Unternehmens weichen die Anforderungen ab, so muss z.B. eine Bank oder eine Versicherung einen umfassenden Schutz gewährleisten.

Um sich vor Bedrohungen zu schützen sind sichere Aufbewahrungsorte der Datenträger und der Server erforderlich, welche nur durch gewisse Personen wie Sicherungsbeauftragter unter Kontrolle einer oder mehreren Person/en betreten werden darf. Sichere Aufbewahrungsorte sind feuerfest, wasserdicht, beständig gegen Erdbeben, gleich bleibende Temperatur / Luftfeuchtigkeit und vor starker elektromagnetischer Strahlung geschützt. Im Normalfall werden die Daten nicht wie oben beschrieben so sorgfältig aufbewahrt, denn es kann sich nicht jede Firma einen extra Raum für die Datensicherung leisten, der temperiert etc. ist. Aber ein regelmässiges Backup ist in jedem Fall wichtig, damit die Daten nicht durch Umwelteinflüsse verloren gehen, oder zumindest bei einem versehentlichen löschen durch einen User rekonstruiert werden können.

Um sich vor Hackerangriffen zu schützen wendet man meistens Hardwarefirewalls an, die nur noch einen gewissen Verkehr zwischen Firmennetz und WAN (z.B. Internet) zulassen um vor Angriffen geschützt zu sein. Firmenintern kann, falls es nötig ist eine Netzwerktrafficüberwachung durchgeführt werden, welche die Mitarbeiter mit deren Wissen regelmässig kontrolliert. Proxy Server und Content Filter schützen den User beim surfen im Internet. Ebenfalls können den Benutzern gewisse Einschränkungen auferlegt werden, wie z.B. die Sperrung einzelner Datenträger im Netzwerk.

Das Thema Viren ist in der heutigen Zeit sehr brisant geworden. Es kommen immer mehr Viren im Internet zusammen, die Schaden anrichten können. Schützen kann man sich mit einem Virenscanner, der fortlaufend aktiv ist und Viren aufspürt. Wichtig ist es, dass der Virenscanner immer auf dem neusten Stand gehalten wird. Heute ist eine Sensibilisierung der Benutzer schon einen grossen Schritt zur Prävention. Es sollte nicht immer jedes File oder Attachement aus dem Internet heruntergeladen und ausgeführt werden.

## 2.5 Backup

### *2.5.1 Wofür wird ein Backup gemacht*

Ein Backup auch Sicherungskopie genannt, wird gemacht um dem Datenverlust vorzubeugen. Datenverluste können durch Umwelteinflüsse (Stromausfall) oder defekte Hardware herbeigeführt werden und sind in den meisten Fällen nicht mehr zu ersetzten. Darum ist es wichtig im privaten- sowie auch im geschäftlichen Bereich regelmässig Datensicherungen durchzuführen.

### *2.5.2 Was gibt es für Backuparten*

Es gibt drei verschiedene Arten ein Backup zu realisieren. Und zwar sind dies die volle-, die differentielle- und die inkrementelle Art. Nun sollte man nur noch wissen, was das alles bedeutet. Also, beim Vollbackup werden immer alle Daten neu gesichert, das heisst es werden alle Daten auf einen Datenträger geschrieben. Beim differentiellen Backup werden alle Daten gesichert, die sich seit dem letzten Vollbackup geändert haben. Und beim inkrementellen Backup werden nur bestimmte mit einem Archivflag markierte Daten gesichert. Diese Archivflags können bei der nächsten Sicherung entweder erhalten- oder gelöscht werden. Außerdem können noch Dateien abhängig vom Dateidatum gesichert werden. Meistens werden mehrere Arten kombiniert zu einem Generationenprinzip.

### *2.5.3 Wie werden Backups durchgeführt?*

Schon seit vielen Jahren werden die Backups in diversen Grossfirmen regelmässig mit einem Bandsicherungsgerät durchgeführt. Jedoch sind neu auch Harddisks zum Zuge gekommen. Es gibt zwei verschiedene Methoden um Sicherungen durchzuführen. Die eine Methode wäre die Sicherungen laufend zu machen, dass heisst die Daten werden auf dem Server abgelegt und gleich auf ein Band oder eine Harddisk dupliziert. Der Vorteil ist, dass bei einem plötzlichen Stromausfall, möglichst viele Daten schon gesichert wurden und nicht verloren gehen. Bei der zweiten Methode werden bestimmte Zeiten festgelegt wann eine Datensicherung stattfinden soll. Der Nachteil hierbei ist, dass bei einem Stromausfall sofort alle Daten gelöscht werden können ohne eine Sicherung gemacht zu haben. Bei allen Bandsicherungsgeräten müssen die Bänder nach einer bestimmten Zeitspanne ausgewechselt werden. In modernen Informatikanlagen gibt es Geräte die die Bänder selbst austauschen können, und so Ordnung halten. Eine Sicherung erfolgt nach dem Prinzip der Attribute. Wenn eine Datei auf dem Server abgelegt wird, sichert ein Sicherungsgerät dieselbe Datei auch gleich noch einmal auf ein Band oder eine Harddisk. Wenn nie etwas an der Datei verändert wird, wird sie auch nie neu gesichert. Jedoch ändert jemand etwas daran wird die Attribute gesetzt und die Datei wird neu gesichert.

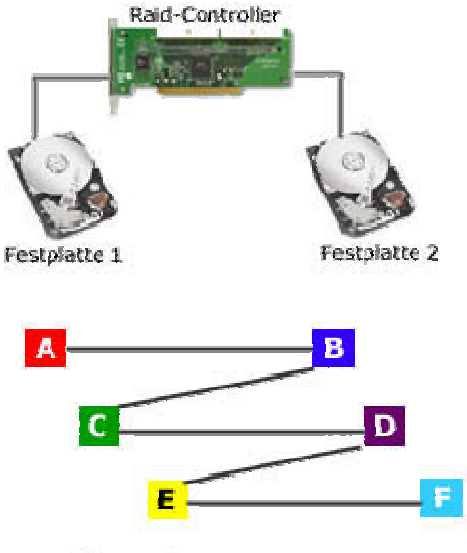
### *2.5.4 Wie könnte ein Backup-Verfahren in der Firma aussehen*

Heutzutage läuft in der Firma die Sicherung automatisch ab. In modernen Sicherungszentralen werden die Bänder automatisch von Robotern ausgetauscht und sauber wieder in einen anderen Schacht versorgt. Es kann sein, dass hier und da mal ein Band ausgewechselt werden muss, aber dies ist eigentlich einer der seltenen Fälle. Die Daten werden vom User zuerst auf ein Serverlaufwerk gespeichert und von dort werden sie an ein Sicherungsgerät gesendet, das die Daten auf die Bänder schreibt. In der Firma werden die Bänder fortlaufend geschrieben, da sonst ein zu grosser Datenverlust entstehen würde bei einer grossen Panne.

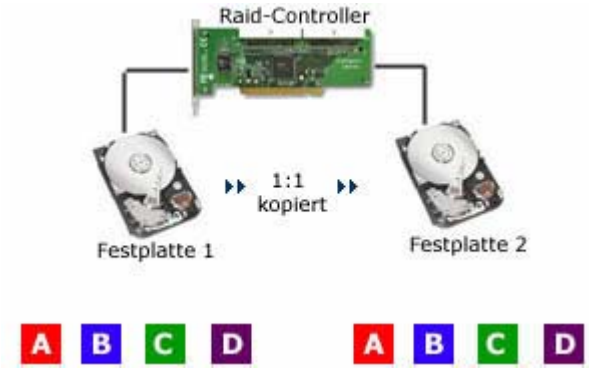
## 2.6 Was ist RAID?

RAID ist eine Abkürzung und steht für Redundant Array of Inexpensive Disks. Mit RAID ist es möglich mehrere Festplatten zusammen zu hängen und diese parallel laufen zu lassen. Somit ist es im Falle eines Datenverlustes möglich die doppelt gespeicherten Daten wieder zurück zu holen. Es gibt 3 verschiedene RAID-Konfigurationen, nämlich RAID 0 RAID 1 und RAID 5.

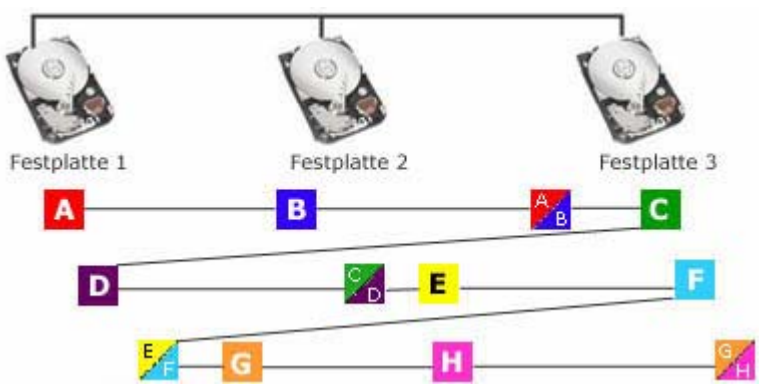
**RAID 0:**
Bei der RAID 0 Konfiguration werden mindestens zwei gleich grosse Festplatten an einen RAID Controller angehängt. Beim speichern werden die Daten dann abwechslungsweise auf beide Festplatten geschrieben. Dies bringt einen grossen Zugriffsvorsprung. Der Nachteil ist jedoch die sehr kleine Datensicherheit. Fällt eines der Laufwerke aus können auch die Daten auf dem anderen Laufwerk nicht mehr verwendet werden, da die Daten auf beide Festplatten verteilt wurden und somit auf dem funktionierenden Laufwerk z.B. Festplatte2, nur die einzelnen Datenteile B,D,F sind.
Die Kapazität der Fastplatten kann zu 100% ausgenutzt werden. Das heisst wenn ich zwei 120 GB Festplatten verwende kann man wie gewöhnlich 240 GB nutzen.




**RAID 1:**
Mit der RAID 1 Konfiguration werden die Daten zuerst auf die eine Festplatte geschrieben anschliessend vom RAID-Controller automatisch auf die zweite Festplatte übertragen. Somit hat man auf beiden Festplatten dieselben Daten und fällt ein Laufwerk aus, können die Daten von der anderen Festplatte zurückgeholt werden. Hat man bei RAID 1 zwei verschieden grosse Festplatten bestimmt die kleinere die effektive Datenkapazität. Werden zwei gleich grosse Laufwerke eingesetzt, können diese maximal ausgenutzt werden. Wenn also zwei 60 GB Festplatten benutzt werden können effektiv 60 GB gespeichert werden und die 60 GB auf der anderen Festplatte werden für die Datensicherung benutzt. Das heisst man hat bei RAID 1 eine höhere Datensicherheit dafür kann nur 50% der ganzen Festplattenkapazität ausgenutzt werden.




**RAID 5:**
Bei den heutigen Serversystemen setzt man meistens die RAID 5 Konfiguration ein. Es werden wie bei RAID 0 mehrere Festplatten zu einem „Netzt“ zusammengehängt, hier sind aber mindestens 3 Laufwerke nötig. Die Daten werden auch wieder in verschiedene Teile unterteilt und abwechslungsweise auf die verschiedenen Festplatten gespeichert. Der entscheidende Unterschied ist, dass bei RAID 5 so genannte Parity-Daten



abgespeichert werden. Dies erlaubt die Rekonstruktion von den Daten auf der ausgefallenen Festplatte.
Beispiel:
Ein ganzes Datenpaket wird in die verschiedenen Teile A und B unterteil. Teil A wird auf die erste Festplatte geschrieben und parallel dazu kann auf Festplatte 2 auch gerade Teil B geschrieben werden, damit ist der Geschwindigkeitsvorteil wieder gegeben. Auf der dritten Festplatte wird die Parity Datei geschrieben. Im Falle das Festplatte 1 oder 2 beschädigt wird können somit mit der Parity-Datei auf der dritten Festplatte die Daten wiedererstellt werden.

# 3 Viren

## 3.1 Was sind Vieren

Immer wieder werden durch die Medien Horrormeldungen bezüglich neuen Viren verbreitet. Es ist schon richtig, dass jeden Monat etwa 100-200 neue Computerviren auf den „Markt“ kommen nur geraten nicht alle in die freie Wildbahn.

In der Umgangssprache wird meistens nur das Wort Virus genannt, wenn man an Programme mit schädlichen Wirkungen denkt. Hiermit sind Viren im eigentlichen Sinne, Trojanische Pferde, logische Bomben und Internetwürmer gemeint. Der Fachmann nennt derartige Programme/Dateien "Malicious" (böswillige Software), kurz gesagt wird jedoch meist von "Malware" gesprochen.

## 3.2 Die Geschichte der Viren

Begonnen hat die Geschichte im Jahre 1986. Mann gelangte zur Erkenntnis, dass es sich bei dem Bootsektor von einer Diskette um einen ausführbaren Code handelt bzw. diesen enthält. So erkannte man, dieser Code kann auch durch ein ausführbares Programm ersetzt werden.

Jedoch ging die Weiterentwicklung zu "fortschrittlicheren" Viren erst 1989 so richtig weiter. So wurden nun auch Viren vorgestellt, die nicht mehr zu reinen Vorführeffekten dienten, sondern zu mehr in der Lage waren. Auch die Anwender wurden jetzt geweckt und wurden auf die Gefahren aufmerksam, die von einem Virus ausgehen können. Ebenso natürlich Unternehmen und Softwareentwickler. Somit brach die Ära der Antiviren-Programme an. 1991 kam Norton Antivirus auf dem Markt. Andere Hersteller folgten innerhalb kürzester Zeit.

Bereits 1992 waren ca. 2000 Viren im Umlauf. Heute werden die Viren nicht wie damals von Diskette zu Diskette übertragen sonder über moderne Medien wie z.B. das Internet.

## 3.3 Virenarten

Unter Virenarten unterscheidet man die verschiedenen Eigenschaften eines Virus. Z.B. er nistet sich im Bootsektor oder in ein Makro ein.

### *3.3.1 ANSI Bomben*

ANSI-Bomben bringen die Tastaturbelegung durcheinander. Wenn z.B. der Benutzer ein v drück erscheit auf dem Bildschirm ein a. Diese Bombe benötigt den ansi.sys Treiber um aktiv zu werden.

### *3.3.2 Construction Kit*

Dies ist nicht direkt ein Virus sonder ein Virenbaukasten. Mit einem solchen Baukasten kann auch ein ganz normaler Benutzer einen Virus generieren, oft sind diese aber primitiv und werden von den Antivirenscanner erkannt.

### *3.3.3 CMOS*

Also CMOS bezeichnet man einen externen Speicher eines Rechners, welcher mit einer Batterie versorgt wird. Er enthält z.B. Informationen wie Uhrzeit und Datum. Ein Virus kann sich nicht in ein solches Bauteil abspeichern, er kann dieses aber löschen oder manipulieren.

### *3.3.4 Companion Viren (Split Viren)*

Diese schon alte Virenart benutzt die Eigenschaft, dass wenn ein Befehl z.B. defrag aufgerufen wird, startet MS-DOS das Programm defrag.exe. Nun ist aber eine Datei mit dem Namen defrag.com vorhanden. Diese wird vor .exe ausgeführt und enthält den schädlichen Code. Oft wird der Benutzer anschliessend zum gewünschten Programm weiter geleitet.

### *3.3.5 Dateiviren*

Diese Art von Viren infizieren nur Dateien. Meist sitzen sie am Anfang an der Datei und springen anschliessend zum Virencode. Dieser wird ausgeführt und das normale Programm wird gestartet. Meist geht die so schnell, dass der Benutzer keine Verzögerung beim starten des Programms wahrnimmt.

### *3.3.6 Dropper / Partitions oder Bootsektorviren*

Bootsektor Viren können normalerweise nicht über ein infiziertes Programm in das System eindringen. Das Programm enthält legendlich den Virencode und installiert den Virus an den gewünschten Ort. Der Virus wird erst nach einem Neustark aktiv. Auch gibt es solche Dropper für Dateiviren, um bei einem Virenscan nicht erkannt zu werden.

### *3.3.7 Direct Aktion Virus*

Diese Art von Viren sind nicht speicherresistent dass heisst sie laufen nicht immer im Hintergrund mit. Sobald der Virus aktiv wird, sucht er sofort nach anderen Programmen die er infizieren kann. Diese Art von Viren erfordert keine hohen Fachkenntnisse darum gibt es auch eine hohe Anzahl dieser Schädlinge, sind aber nicht sehr weit verbreitet.

### *3.3.8 Fast Infector*

Schon durch das Öffnen oder Schliessen einer Datei, werden diese durch einen solchen Virus infiziert. Startet der Anwender einen Virenscan so sind alle jemals geöffneten Dateien infiziert. Dieser Virus ist leicht zu erkennen, da er das System stark abbremst.

### *3.3.9 Hoaxe*

Ein Hoaxe ist kein Virus sondern nur ein schlechter Scherz. Man Bezeichnet damit Virenwarnungen, die das Postfach fast überschwemmen. In der Realität ist gar kein Virus vorhanden.

### *3.3.10 HTML Viren*

Im Oktober 1998 wurde erstmals ein HTML-Virus publik. Zu dieser Zeit hatte man dies nicht für möglich gehalten. Dieser Virus nistet sich als ein VB-Element in einem HTML Dokument ein.

### *3.3.11 Kernel Viren*

Diese Sorte von Viren infiziert zuerst bestimmte Dateien des Betriebssystems. Z.B. unter MSDOS die Datei io.sys. Aktuell sind nur wenige solche Viren bekannt.

### *3.3.12 Killerprogramme*

Unter Killerprogramme versteht man Viren, welche nach einer Anzahl von Aktionen ein Ereignis oder eine Aktion auslösen. Diese Viren besitzen einen internen Zähler und warten bis dieser 0 erreicht hat. Anschliessend führen sie eine Aktion aus wie das Löschen von Daten oder der Festplatte.

### *3.3.13 Makroviren*

Makroviren infizieren keine Programm sonder Dokumente wie z.B. .doc oder .xls. Wer kein Word oder Excel installiert hat, hat nichts von solchen Viren zu befürchten. Makroviren sind mächtig, weil sie die Möglichkeit haben die Funktionen der Programmiersprache VB auszunutzen.

### *3.3.14 Polymorphe*

Früher reichte es aus die Bit und Bytefolge eines Virus zu analysieren und die Virensignaturdatei dementsprechend zu ergänzen. Dies haben aber auch nicht die Virenbastler verschlafen. Der Quellcode des Virus wird verschlüsselt und somit ist die Antivirensoftware mit einem anderen Code konfrontiert.

### *3.3.15 Retroviren*

Retroviren greifen direkt die Antivirensoftware an. Das Ziel ist diese völlig ausser Kraft zu setzen, damit sich der Virus den eigentlichen Sinn und Zweck ungehindert auf dem System ausführen kann.

### *3.3.16 Script Viren*

Diese Art von Viren bedient sich der Scriptsprachen wie z.B. VB. Der Virus infiziert z.B. alle Dateien im Browser Cache. Erscheinen plötzlich komische Icons oder sonstige Bilder auf dem Desktop ist dies ein typisches Beispiel für ein Script Virus.

### *3.3.17 TSR Dateiviren*

Diese Art von Viren ist sehr häufig anzutreffen. Sie infizieren .exe und .com Dateien, jedoch gibt es auch einige die Gerätetreiber oder Überlagerungsdateien infizieren. Er ist im Hintergrund immer aktiv und wartet, bis der Anwender ein nicht infiziertes Programm öffnet um dies zu befallen.

### *3.3.18 Update Viren*

Dies kann ein einfacher Dateivirus mit einer Update Funktion sein. Der Virus überprüft, ob schon eine neuere Version von ihm vorhanden ist. Sind jedoch die Infizierten Dateien Ursprung einer älteren Version, infiziert er diese neu.

### *3.3.19 Überschreibende Viren*

Diese Viren sind sehr klein und zugleich gefährlich. Es gibt Versionen mit der Grösse von nur 23 Byte hingegen richten sie immer Schaden auf dem Infizierten System an. Sie überschreiben Dateien meist aber nur in ihrem aktuellen Verzeichnis.

### *3.3.20 Zeitzünder, Logische Bomben*

Dieser Virus ist darauf Programmiert oft an einem bestimmten Datum eine Aktion auszuführen. Z.B. starten sie dann einen Angriff auf einen Webserver oder löschen sich selbst und die Festplatte mit. Diese Art von Viren reproduziert sich nicht

### *3.3.21 Trojanisches Pferd*

Eigentlich ist die Geschichte von Trojanischen Pferd in die Geschichte einzuordnen. Ein Trojaner nistet sich in ein System ein und öffnet eine Hintertür für den Programmierer. Je nach Trojaner erhält so der Programmierer die Kontrolle über das infizierte System. Eigentliche schädliche Routinen laufen nur im Hintergrund ab.

### *3.3.22 Würmer*

Würmer sind sehr gefährlich, weil sie sich sehr schnell selbst verbreiten ohne dass der Benutzer aktiv werden muss. Eine typische Verbreitung geschieht durch E-Mail bzw. durch das Adressbuch des infizierten Systems.

Oftmals kombiniert ein Virus mehrere Typen.

## 3.4 Massnahmen gegen Viren und andere Schädlichen Programmen

Die Virenprogrammierer sind meistens den Antivirensoftware Hersteller einen Schritt voraus. Spielen wir folgendes Szenario durch: Ein neuer Wurm verbreitet sich über den gesamten Globus. Der Antivirensoftwarehersteller muss zuerst diesen Virus analysieren und die Signatur der Viren Definitions- Datei hinzufügen. Anschliessend muss diese Datei unter den Benutzern verteilt werden. Bis jeder User gegen die neue Bedrohung geschützt ist, dauert es oft einige Tage. In dieser Zeit verbreitet sich der Wurm rapid.

Wirklich sicher ist nur ein Inselsystem, ohne irgendwelche Anschlüsse zur Aussenwelt oder mobilen Datenträgern. Ansonsten empfehlen sich eine Antivirensoftware und eine Personalfirewall. Die Voraussetzung ist, dass die Produkte regelmässig am besten täglich aktualisiert werden. Warum eine Firewall? Personalfirewalls sind in der Lage gefährliche Elemente im WEB wie z.B. ActiceX Elemente oder VB-Elemente zu blocken.
All diese Massnahmen setzen einen informierten Benutzer voraus. So sollten nicht E-Mail Attachements geöffnet werden oder wahllos Dateien heruntergeladen und ausgeführt werden. Auch setzt dies die richtige Konfiguration des Browser voraus.

## 3.5 Wie entferne ich Viren

Da viele Viren im Internet kursieren gibt es nicht genau eine Anleitung. Ich kann hier legendlich die allgemeine Vorgehensweise aufzeigen. Nehmen wir an mein Antivirenprogramm hat einen Virus auf dem System entdeckt:

- Zuerst heisst es Ruhe bewahren und nicht wie wild durch sämtliche Optionen klicken
- Bei einer Infizierung einer Programmdatei sollte die Datei gelöscht werden (nicht repariert) und anschliessen von der CD wieder aufgespielt.
- Handelt es sich um ein Dokument und es steht kein Backup zur Verfügung, sollte die Datei bereinigt werden. Dies kann aber zu Fehlern führen, da manchmal Teile des Virus davon kommen und weitere Fehlalarme auslösen.
- Wurde eine Systemdatei infiziert, sollte man zuerst eine Virenbeschreibung lesen und nach einem Entfernungstool z.B. auf http://www.symantec.com suchen

Bei der Infizierung durch ein Bootsektorvirus sieht dies ein wenig schwieriger aus.

- Lesen sie zuerst die Beschreibung zum Virus

- Falls noch Zeit ist, sichern Sie ihre Daten
- Anschliessend starten Sie Ihren PC durch das verwenden der Resettaste neu. Dies könnt zur Folge haben, dass der Virus noch im Abreisspeicher war und keine Gelegenheit gefunden hat sich einzuschreiben.
- Entfernen Sie nun den Virus mit Hilfe der Notfalldiskette ihres Antivirenproduktes

## 3.6 Wie funktioniert ein Virenscanner

Prinzipiell unterscheidet man von der heuristischen und der Sand Box Methode neben der normalen Plattendurchsuchung. Diese Technik wird jedoch laufend verfeinert, neue Verfahren erhöhen die Erkennungsrate.

### *3.6.1 Guard*

Unter einem Guard versteht man einen Wächter der den PC zu seinen Betriebszeiten überwacht. Das Ziel ist Dateien zu erkennen die geöffnet, geschlossen oder bearbeitet werden, welche durch ein schädliches Programm infiziert sind. Die Daten werden einfach nach bekannten Signaturen durchsucht und mit der Datenbank verglichen. Dies ist auch der Grund warum beim verwenden eines aktiven Antivirenprogrammes Performance Verluste eintreten können.

### *3.6.2 Durchsuchen der Platte*

Hier werden sämtliche Dateien auf der Festplatte durchsucht nach bekannten Signaturen und Merkmale von schädlichen Programmen. Diese Informationen werden wieder mit der so genannten Virendefinitionsdatenbank verglichen und allfällig Alarm ausgelöst.

### *3.6.3 Die heuristische Methode*

Ich möchte diese Methode anhand eines Beispieles zeigen. Nehmen wir an eine Datei enthält folgender Inhalt:

```
If System.PrivateProfileString(“”,
 “HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security“,
“Level“) <>“”
Then
 Command Bars(„Macro“)…….
```

Nun durchsucht das Antivirenprogramm dieses File und bildet eine so genannte Checksumme. Wenn die Checksumme einen gewissen Wert überschreitet wird Alarm ausgelöst. In unserem Fall sollte dies geschehen, weil es sich um einen Ausschnitt des Melisa Wurmes handelt. Diese Methode kann auch zum erkennen von noch unbekannten Viren verwendet werden.
Bei dieser Technik ist es schwierig den Checksummenwert so fest zu legen, dass keine Fehlalarme ausgelöst werden oder Viren nicht erkannt werden.

### *3.6.4 Sandbox*

Auch die Sandbox wird zur Erkennung von noch nicht bekannten Viren und Würmer verwendet. In diesem Fall simuliert die Antivirensoftware den gesamten PC inklusive Hardware um die Reaktion des Virus zu testen. Nun wird diesem Wurm oder Virus innerhalb der Sandbox freien lauf gelassen. Bösartige Absichten werden somit unmittelbar erkannt.

# 4 Datenschutz

## 4.1 Definition Datenschutz

Mit Datenschutz bezeichnet man die Geheimhaltung persönlicher Angaben die z.B. bei einer Firma gespeichert sind und nicht an dritte weitergegeben werden dürfen.

## 4.2 Wo wird der Datenschutz definiert

Der Datenschutz ist in der Bundesverfassung Artikel 13, Absatz 2 definiert.
Auszug aus der Bundesverfassung Art.13[2]:

- Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten

# 5 Kryptographie

## 5.1 Was versteht man unter Kryptographie

Heutzutage findet man Kryptographie überall von der Passwort Kodierung, zu verschlüsselten E-Mails, von IPSec zum VPN und sogar zum verschlüsselten Dateisystem.
Die Datensicherheit ist der Grund dafür, dass sich Menschen für die Datenverschlüsselung entschieden haben. Im Allgemeinen ist Kryptographie der Sammelbegriff für alle Verfahren, um Daten zu verschlüsseln oder auch Passwörter sicher abzuspeichern. Es gibt verschiedene Veschlüsslungsverfahren, auf welche ich weiter unten noch eingehen werde. Dabei werden die Daten z.B. vertausch, ausgetauscht oder geändert. Die Daten werden unter der Verwendung eins so genannten Algorithmus verschlüsselt. Heute gibt es einige wenige Algorithmen, welche mehrere Jahre zur Entschlüsslung der Daten brauchen würden.

## 5.2 Einen Abstecher in die Geschichte der Kryptographie

Schon zu der Zeit von Cäsar wurde die Kryptographie im einfachsten Rahmen angewandt. Die so genannte Cäsar-Chiffrierung funktioniert einfach: Man verschob jeden Buchstaben um 3 Buchstaben weiter im Alphabet. So wurde aus einem S ein V, E zu H usw. Nach heutigen Massstäben war diese Technik sehr einfach aber Cäsar reichte die damals vollkommen aus. In der Tat wird ROT13 (rotiere 13), eine Technik die viel Ähnlichkeit zur Cäsar Chiffrierung aufweist, heute noch eingesetzt. Natürlich nicht, um Informationen vor anderen Menschen geheim zu halten, sonder eher, um niemand zu beleidigen wenn man Witze überträgt. ROT13 ist so einfach, dass man es nur mit Papier und Bleistift entschlüsseln kann. Am Besten schreibt man zwei Reihen nebeneinander auf. Wobei die zweite Reihe um 13 Stellen Verschoben ist:

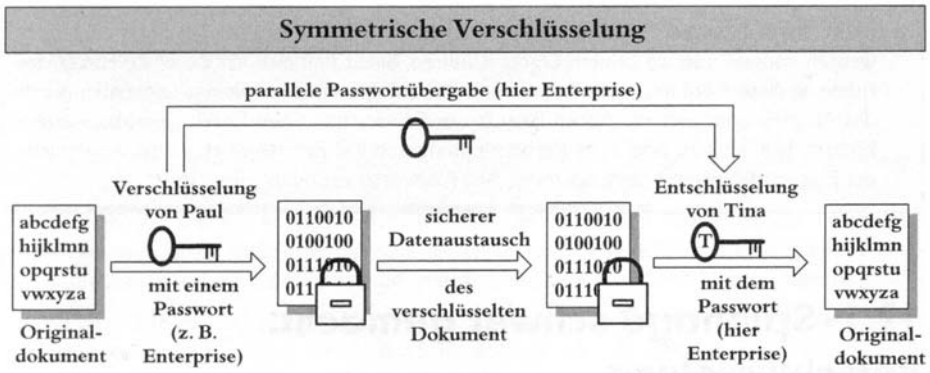
A N
B O
C P
Usw.

## 5.3 Schlüsseltypen

Verschlüsslung ist nicht gleich Verschlüsslung und es gibt eine Unzahl von Verfahren, die mehr oder weniger den Daten des Nutzers ausreichend Schutz bieten. Jede Methode basiert auf einem mathematischen Algorithmus, der je nach Ausführung für den Computer einen erheblichen Rechenaufwand bedeutet. Dem Anwender bringt ein absolutes sicheres Verfahren, das Stunden oder Tage dauert, nicht sehr viel Nutzen. Zu den schnellen Techniken zählen die symmetrischen Systeme, während die asymmetrischen Algorithmen eher zu den langsameren gehören.

### *5.3.1 Symmetrische Verschlüsslung*

Bei einer symmetrischen Verschlüsslungstechnik werden die Klartextdaten einfach mit einem Generalschlüssel oder einem individuellen Passwort kodiert und damit für Unbefugte unleserlich.




**1) Datenaustausch einer Datei mithilfe eines symmetrischen Verschlüsslungsverfahrens**

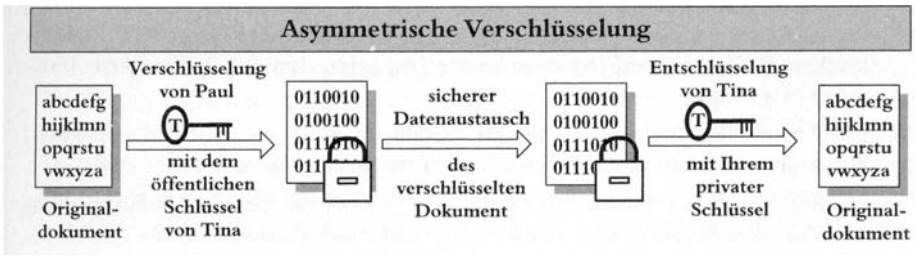
Jeder im Besitz diese geheimen Schlüssel (Secret Key) ist, kann die Daten wieder entschlüsseln und lesen. In unserem Beispiel das Passwort Enterprise. Hier liegt auch der wesentliche Nachteil dieses Verfahrens, weil jeder berechtigte Nutzer den Schlüssel kennt und an Dritte weitergegeben werden kann. Schon bei der Übertragung des Schlüssels besteht ein hohes Risiko. Z.B. kann die Übertragung zwischen Server und Client belauscht werden und somit den geheimen Schlüssel in Erfahrung gebracht werden. Darum kommt bei einer Schlüsselübertragung oft wieder ein asymmetrisches Verfahren zum Einsatz.

**DES** (Data Encyption Standard): Dieser Algorithmus wird oft im Bereich der Finanzbuchhaltung eingesetzt und fast als Standart bezeichnet. Obwohl nunmehr als 20 Jahre im dauerhaften Einsatz getestet und ununterbrochen analysiert, wurden bis heute keine grösseren Schwächen im Algorithmus aufgedeckt. Das Problem beim DES besteht in der geringen Schlüsselstärke von 56 Bit (8Byte), was mit heutigen Rechnern in angemessener Zeit durch eine Brute Force Attacke geknackt werden kann. Um weiterhin dem notwendigen Sicherheitsanspruch gerecht zu werden, wurde die Schlüsselstärke auf 168 Bit (3DES) angehoben. Wie dieser Algorithmus funktioniert würde den Rahmen dieser Dokumentation sprengen.

Weitere symmetrische Algorithmen sind AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish und Twofish.
Die bekanntesten und am meisten Eingesetzten Algorithmen sind hier wohl 3DES, AES und IDEA.

### *5.3.2 Asymmetrische Verschlüsslung*

Das asymmetrische Verfahren wird auch als Public Key-Verfahren bezeichnet, indem der öffentliche Schlüssel zum Verschlüsseln der Daten im Gegensatz zum Secret-Key Verfahren nicht geheim ist.
Der wesentliche Vorteil ist, dass der Schlüssel aus einem Public Key (nicht geheim), mit dem Daten verschlüsselt werden können und einem Secret Key (geheim) mit dem Daten wieder entschlüsselt werden besteht. Dadurch ist keine Übertragung des Schlüssels notwendig. Wie auch beim symmetrischen Verfahren existieren hier auch mehrere Algorithmen.




**2) Asymmetrisches Verfahren**

RSA (Rivest Shamir Adelmann) das wohl bekannteste Verfahren der Firma RSA Data Security Inc. das über die Jahre hinweg am besten getestet wurde. Ab einer Schlüsselstärke von 1024 Bit besteht mit der zurzeit verfügbaren Rechenleistung keine Chance zum Knacken des Codes. Der Algorithmus war bis zum 20. September 2000 in den USA patentrechtlich geschützt, ist aber leider nicht frei verfügbar. Dieses Verfahren wird z.B. in der Verschlüsslungsoftware PGP verwendet.

Andere Algorithmen sind z.B. Diffie-Helmlmann, DSS und ELGamal.

## 5.4 Verschlüsslungssoftware

Es gibt unzählige Produkte in diesem Bereich. Einige kostenlos andere kommerziell. Leider bieten aber nicht alle Produkte den Selben Schutz.

### *5.4.1 PGP*

Die wohl populärste Software ist PGP (Pretty Good Privacy) und heisst auf Deutsch etwa „recht gute Privatsphäre“. Phil Zimmermann hat erstmals im August 1991 PGP veröffentlicht und hatte dem Public-Key-Verfahren den Aufschwung erteilt. In der zwischen Zeit wurde die Software mehrmals von verschiedenen Organisationen verbessert und veröffentlicht. Es gibt sowohl kommerzielle wie kostenlose Versionen für nicht kommerzielle Zwecke. Ab dem März 1998 wurde die Entwicklung von McAfee weitergeführt, wobei eine Freewareversion für den Privatanwender angeboten wurde. Zu diesem Zeitpunkt hat sich die US-Regierung bzw. die NSA stark dafür eingesetzt, eine Hintertür in PGP einzubauen. Die Umsetzung wird zwar bestritten, aber durch die teilweise Geheimhaltung des Quellcodes konnte bisher nichts nachgewiesen werden. Dies war auch der Zeitpunkt, bei welchem Phil Zimmermann aus dem Projekt ausgestiegen ist. McAfee hat nach der Version 7.1 die Weiterentwicklung eingestellt und nach der Abtrennung gewisser gewinnbringenden Teile den Verkauf eingeleitet. Mittlerweilen hat die Firma Network Associates im Juni 2002 die Schulden von PGP übernommen und die Version 8.0 angekündigt. Mehr zur aktuellen Version ist auf der Homepage http://www.pgp.ch zu erfahren.

#### 5.4.1.1 Wo wird PGP eingesetzt

PGP ist ein Programm für die Verschlüsselung von Nachrichten. Richtig eingesetzt, schließt es die Möglichkeit, per E-Mail oder Diskette versandte Daten ohne Berechtigung zu entschlüsseln,

weitgehend aus. Es ist aber kaum dazu geeignet, Daten auf einem Computer in komfortabler und zuverlässiger Weise vor fremdem Zugriff zu schützen.

#### 5.4.1.2 Welche Techniken setzt PGP ein?

PGP ist das wohl bekannteste Programm zur asymmetrischen Verschlüsselung. Dabei setzt PGP eigentlich auf verschiedene Verschlüsselungstechnik. Da das Public-Key-Verfahren viel Rechenzeit benötigen, kombiniert PGP eine asymmetrische RSA-Verschlüsselung mit einer symmetrischen IDEA-Verschlüsselung. Auch wird ein so genannter Session Key hinzugefügt und im IDEA Algorithmus verschlüsselt. Ein Session Key ist nur für eine Verschlüsslung bzw. eine Sitzung gültig und bietet somit mehr Schutz. Ich möchte an dieser Stelle nicht weiter in das Verfahren eingehen, weil dieses Thema schnell unübersichtlich wird.

### *5.4.2 SaveGuard PrivateCrypto*

Ein sehr einfach gehaltenes Verschlüsslungsprogramm von Utimaco Saveware ver- und entschlüsselt Dateien nach dem AES Algorithmus. Es ist dabei in der Lage selbstentschlüsselnde Archive zu erstellen, sodass der Empfänger nicht über das eigentliche Programm verfügen muss. Mehr Informationen gibt es unter http://www.utimaco.de .

# 6 Urheberrecht

## 6.1 Urheberrecht

Das Urheberrecht gibt dem Urheber, also derjenigen natürlichen Person die das Werk erschaffen hat, das Recht ob, wann, wie und unter welchem Namen das Werk veröffentlicht wird. Als Werk wird alles bezeichnet das eine natürliche Person erschaffen hat und weiter verwendet werden kann. Also auch schon Computerprogramme, Entwürfe, Titel oder sogar Pantomimen werden als Werk betrachtet und werden Urheberrechtlich geschützt. Der Urheber kann entscheiden ob und wie das Werk nach der Veröffentlichung weiter verbreitet werden soll. Würde also ein Urheber eines Songs sagen, dass einer seiner Songs auch im Internet verbreitet werden darf wäre das downloaden dieses Songs nicht verboten. Nun, weil so der Urheber keinen Gewinn machen würde macht er dies sehr wahrscheinlich nicht, somit ist das downloaden verboten weil es durch das Urheberrecht geschützt ist.
Das Urheberrecht erlischt für Erfinder von Computerprogrammen 50 Jahre nach dem Tod des Erfinders und für sonstige Werke erhält das Urheberrecht bis 70 Jahre nach dem Tod des Urhebers.
Nicht Urheberrechtlich geschützt sind Gesetze, Verordnungen, amtliche Erlasse, Entscheidungen, Protokolle, Zahlungsmittel und so weiter. Diese „Werke“ dürfen also unbeschränkt verbreitet und weitergegeben werden.

## 6.2 Softwarelizenzen

Weil nach unserem Urheberrecht auch ein Computerprogramm als Werk der Literatur, Wissenschaft und Kunst zählt, muss auch hierfür bezahlt werden sofern das der Urheber verlangt. Das bezahlen geschieht nicht durch das verkaufen des Programms sondern durch das lizenzieren des Programms. Weil man nur mit dem Kauf einer Software ein Vertrag für die Nutzungsbedingungen nicht rechtsgültig ist, muss man dies mit dem Kauft der Lizenz machen.
Kauft man sich also in einem Laden irgendeine Software bezahlt man nicht für die Software selbst, diese wäre nämlich gratis. Die Software darf aber einfach so nicht benutze werden. Um sie zu benutzen muss man sich eine Lizenz kaufen, das ist dann eben der Preis den man im Laden bezahlt. Mit einer normalen Lizenz ist es erlaubt die Software zu benutzen und für sich selbst eine Sicherheitskopie anzufertigen. Wird eine Software von mehreren Usern benutzt müssen spezielle Lizenzen gekauft werden die das Benutzen für mehrere User erlauben. Es gibt auch so genannte Gruppenlizenzen die man zum Beispiel in kleineren Firmen oft kauft. Mit die-

sen Lizenzen ist es möglich einfach für einen ganzen Computerraum eine Lizenz zu kaufen. Für grosse Firmen und so weiter gibt es sogar Lizenzen die eine unbegrenzte Anzahl von Benutzern zulassen, Diese Lizenzen werden Master-Lizenzen genannt. Für Schulen und ähnliche Einrichtungen gibt es oft auch spezielle Schul-Lizenzen. Diese sind billiger und meistens auch für eine unbegrenzte Anzahl von Benutzern gedacht. Laut Lizenzrecht dürfen solche Lizenzen aber ausschliesslich nur für Lernzwecke gebraucht werden.

## 6.3 Was sind:

### *6.3.1 Freeware/Shareware – Rechte*

Ein Freeware Programm darf man so oft man möchte kopieren und weitergeben. Das einzige was mit einem Freeware Programm verboten ist, ist das Programm nach eigenen Wünschen abzuändern. Damit würde man gegen das Urheberrecht verstossen. Will mach ein Programm abändern müsste der Quellcode vom Urheber gekauft werden. Hin und wieder möchten die Autoren dieser Programme eine Postkarte als Belohnung (cardware), oder sie ermutigen den Benutzer, falls ihm das Programm gefällt, eine kleine Spende zu machen (donationware), es darf aber nicht Bezahlung verlangt werden.
Free Software, Open Source Software oder Public Domain Software ist nicht das Selbe. Diese Programme sind nicht alle kostenlos. Sie können gratis sein es darf aber auch dafür verlangt werden. Bei diesen Programmen steht nur de Quellcode frei zur Verfügung und dieser darf hier auch abgeändert werden.
Shareware kann erst einmal gratis ausprobiert werden. Dieses Ausprobieren ist entweder zeitlich eingeschränkt (nur 30 Tage oder nur x-Programmstarts), oder von dem Programm steht nur ein Teil zur Verfügung (z.B. die ersten 5 Level von einem 20-Level-Spiel). Auch Shareware darf frei weitergegeben werden wie Freeware. Meistens ist es bei Shareware Programmen möglich sich eine Lizenz zu kaufen mit welcher das Programm uneingeschränkt genutzten werden kann.

### *6.3.2 Raubkopien*

Egal ob man Raubkopien verkauft, anfertigt oder sie selbst braucht und egal ob privat oder im Unternehmen jeder der was mit Raubkopien zu tun hat muss mit einer Strafrechtlichen Verfolgung rechnen. Mit Raubkopien verstösst man gegen das Urheberrecht und muss somit Geldbussen bis zu 40000.-Fr oder einer Freiheitsstrafe von einem Jahr in kauf nehmen, bei gewerblichem Verstoss gegen das Urheberrecht stehen sogar Busen bis 100'000.- sFr und bis zu 3 Jahren Gefängnis an. Dazu muss mit einer Schadensersatzklage gerechnet werden.
Im Falle eines Gerichtlichen Verfahrens müssen die Verfahrenskosten natürlich auch noch vom Angeklagten übernommen werden.

# 7 Schlusswort

Ich hoffen wir konnten Ihnen einen kleinen bzw. möglichst grossen Einblick in die riesengrosse Welt des Datenschutzes und der Datensicherheit geben. Sehr wahrscheinlich wird dies auch immer ein grosses Thema bleiben bei welchem man immer auf dem neusten Stand sein sollte. Auch das Urheberrecht wird in der heutigen Zeit mit den Musik-Downloads immer wichtiger, bei jedem Download eines urheberrechtlich Geschützten Titel, muss man mit den entsprechenden Konsequenzen rechnen.

# 8 Quellen

## 8.1 Datensicherheit und Datenschutz

Bundesverfassung: Art. 13²
www.net-lexikon.de/Datensicherheit.html
www.computerlexikon.com/begriff.php?id=172
www.inf.tu-dresden.de/~lvinfhl4/download/dsds/1_einfuehrung.pdf

## 8.2 Backup

www.speicherguide.de/magazin/special1003.asp?theID=183&todo=1
www.gera-web.de/opencms/export/geraweb/hp/produkte/sicherheit/backup.html
www.winscore.at/download/doku/Backup-Experte.pdf

## 8.3 Viren und Trojaner

Die Hacker Bibel: Ryan Russle, mitp, S.41, S141 bis 204
Intern: Marc Ruef, DATA BECKER, 2003, S.570, S.595, S.749 bis 763, S.790 bis 807
www.trojaner-info.de/viren/virentypen.shtml
www.trojaner-info.de/viren/virenwas.shtml
www.pcwelt.de/ratgeber/viren/16656/9.html
www.computec.ch/
www.geocities.com/Athens/1802/ger_pgpdoc1.html#5.4

## 8.4 RAID

www.pc-erfahrung.de/Index.html?Raid.html

## 8.5 Urheberrecht

www.admin.ch/ch/d/sr/231_1/index.html#id-2

## 8.6 Softwarelizenzen

http://ig.cs.tu-berlin.de/w2000/ir1/referate1/k-1b/swlicense.html
www.vip7.de/info/presentation/develop/softwarelizenzen.htm

## 8.7 Raubkopien

http://global.bsa.org/switzerland/piraterie/konsequenzen.php

# 9 Glossar

| | |
|---|---|
| **Integrität** | Integrität bedeutet, dass an einem System nur erlaubte und erwünschte Veränderungen an den dort enthaltenen Informationen vom User zugelassen werden. |
| **Algorithmus** | Ein Algorithmus ist ein mathematisches Verfahren welches ausgeführt wird anhand der Regeln des Algorithmus. In der Kryptographie ist dies wie eine Formel zur Verschlüsslung. |
| **Kryptographie** | Sehen Sie den Abschnitt „Was ist Kryptographie?“ |
| **Sandbox** | Ein simulierter Rechner inklusive Betriebssystem und Hardware. |
| **Virendefinitionsdatenbank** | Jedes Antivirenprogramm besitzt eine solche Datenbank. Hier sind Merkmale und Signaturen von den bekannten Viren eingetragen. |