

Dossier

Sicherheit im Bildungswesen

## 1 Definition: Was ist Sicherheit?

Es gibt einige Definitionen von Sicherheit, je nachdem von welcher Fachrichtung man ausgeht. Im Bereich der IT-Sicherheit haben wir es jedoch nicht mit Sicherheit im mathematischen Sinne ( $p=1$ ) zu tun, sondern eher mit einer subjektiven und nur sehr schwer messbaren Sicherheit.

In unserem Falle könnte man Sicherheit definieren als "In Erfahrung gegründetes und sich bestätigendes Gefühl, von gewissen Gefahren nicht vorrangig getroffen zu werden".

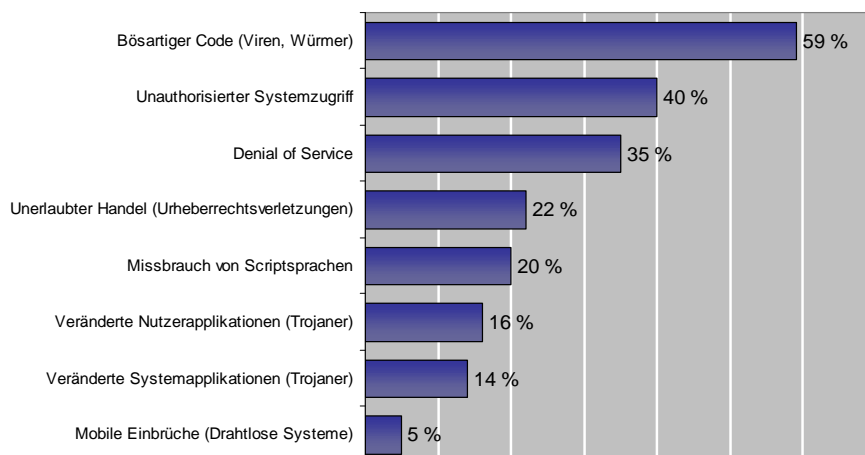
Sicherheit kann nicht umfassend und ohne Ambiguität definiert werden. Gerade deshalb ist es wichtig die Grundsätze der IT-Sicherheit zu kennen:

- Es gibt keine 100%ige Sicherheit
- Sicherheit kann nie bewiesen werden, sondern nur Unsicherheit
- Sicherheit ist nicht das Ziel, sondern der Weg
- Schutzmassnahmen sind eine Kosten-/Nutzenrechnung: Gegen wen will ich meine Informationen schützen und was ist sie uns / einem Angreifer wert?
- Eine Schutzmassnahme sollte nicht mehr kosten als das, was ich schützen will wert ist (können auch subjektive Werte sein)
- IT-Sicherheit wird beeinflusst durch Menschen, Prozesse und Technologie

Die starke Verbreitung des Internet und der breiteren Verfügbarkeit von Hackerwissen hat dazu beigetragen, dass ein Angreifer heutzutage wenig Aufwand hat um Angriffe starten zu können. So enthalten vermeintlich uninteressante Ziele bereits ein Angriffspotential, weil es schlicht trivial geworden ist, toolbasierte Hackerangriffe über das Internet zu starten.

## 2 Gefahren / Problemfälle

Neben dem eher romantischen Bild des Hackers als rebellischem Teenager, der ins Schulsystem einbricht um seine Noten aufzubessern, bedeuten solche Aktivitäten heute eine ernstzunehmende Gefahr für Bildungsstätten aller Stufen. Attacken oder Missbrauch von Informatik-Sachmitteln können sich auf verschiedene Arten darstellen. Die nachfolgende Grafik zeigt eine prozentual gegliederte Zusammenstellung der Angriffs- und Missbrauchsarten im Jahre 2003:



### 2.1 Hackermethoden

Hackermethoden gibt es viele. Je nach Kenntnisstand, steht dem Angreifer eine Vielzahl von Möglichkeiten und Tools zur Verfügung. Diese Darstellung erhebt keinesfalls den Anspruch auf Vollständigkeit und soll nur einen kleinen Einblick erlauben.

Informationen über die Funktionsweisen des Internet und verwandter Dienste sind öffentlich und somit für jedermann frei zugänglich. Neben der "zivilen" Nutzung dieser Informationen stehen diese natürlich auch für Hacker offen. Mit dem grundsätzlichen Verständnis um die Funktionsweise des Internet wurden auch bald einmal dessen Schwächen offensichtlich – nämlich das Fehlen von jeglichen Sicherheitsfunktionen. Viele der damals eingeführten Protokolle, welche auf der Internet-Grundlage Transport Control Protocol / Internet Protocol (TCP/IP) basieren, kränkeln ebenso an einem Mangel von Sicherheit.

Nehmen wir als Beispiel die folgenden Protokolle:

- FTP (Transfer von Dateien)
- HTTP (Transfer von Webseiten beim Surfen)
- SMTP (Senden von Email Nachrichten von A nach B)
- POP (Abholen von Email Nachrichten vom Postfach)
- Telnet (Fernwartung von Rechnern)

Alle oben erwähnten Protokolle haben eines gemeinsam: Sie übertragen Benutzernamen und Passworte im Klartext über das Internet.

#### 2.1.1 Sniffing

Wie oben beschrieben übertragen die am häufigsten gebrauchten Internet-Protokolle Anmeldeinformationen im Klartext über das Internet – was uns zur wohl einfachsten Möglichkeit eines "Hacking" bringt. Ein geneigter Hacker muss lediglich mit einem "Sniffer" (Netzwerk-Abhörsoftware) an geeigneter Stelle mithören und kann so fast komplett ohne Aufwand Benutzernamen und Passworte problemlos abhören. Neben Standardmässigen Sniffern, welche hauptsächlich für die legitime Fehlersuche im Netzwerk gedacht sind, gibt es auch spezialisierte Hackertools – welche speziell auf Benutzernamen und Passworte im Datenstrom hören und diese gezielt herausfiltern. Natürlich kann man solche Tools auch nutzen um im eigenen Netzwerk zu testen, inwiefern Passworte unverschlüsselt übertragen werden.

#### 2.1.2 Malcode

Unter "Malcode" (Malicious Code) werden im Allgemeinen "böartige" Programme verstanden, welche in Form eines Virus, eines Wurms oder eines Trojaners vorkommen können. Natürlich sind auch Kombinationen möglich. Viren und Würmer sind meist nur ärgerlich, können aber auch handfesten Schaden verursachen. Nicht nur durch die blosser Verbreitung und eine eventuell damit ausgelöste "Denial of Service" Attacke, sondern auch durch die Möglichkeit, dass Viren einen Trojaner als blinden Passagier mitführen. Ist ein Trojaner einmal im System, kann er dem Angreifer den kompletten Systemzugriff ermöglichen. Bekannte Vertreter dieser Trojanerkategorie wären "SubSeven", "Back Orifice" und einige andere. Laut einer aktuellen Gartner-Studie sind 59% aller befragten Betriebe regelmässig von Malcode-Attacken betroffen.

### 2.1.3 Ausnutzen von Software- und Konfigurationsfehlern

Ein sehr grosses Problem beim Einsatz von Computern ist deren Komplexität geworden. Mit jeder neuen Version wird Software mit neuen Funktionen ausgestattet, was auch bedeutet, dass neue mögliche Angriffspunkte entstanden sind. Bereits muss ein relativ grosser Aufwand betrieben werden um Systeme sicher zu machen und auch sicher zu halten.

Ein Grossteil der unautorisierten Zugriffe auf ein System kommt zu Stande weil ein Angreifer gezielt eine Schwäche (Vulnerability) eines Betriebssystems oder einer Applikation nutzt. Obwohl viele Hersteller meist umgehend Korrekturen von bekannten Schwächen zur Verfügung stellen, bleibt immer noch ein mehr oder weniger grosses Zeitfenster für einen Angriff offen. Von der Meldung einer Schwäche an den Hersteller bis zur Installation einer Abhilfe auf einem Kundensystem vergehen Wochen bis Monate. Ganz zu schweigen von den Schwachstellen die nicht bekannt sind. Man kann sich zum Beispiel fragen, wann (wenn überhaupt) ein Hacker eine gefundene Schwachstelle dem Hersteller bekannt gibt. Vermutlich dann wenn er sie selbst ausgiebig genutzt hat.

Die am häufigsten angetroffene Ursache für unerlaubten Zugriff ist jedoch eine mangelhafte Konfiguration von Systemen und die Nichtbeachtung von Sicherheitsratschlägen in den Software-Handbüchern. Software wird oft mit Standard-einstellungen (off auch Standard-Passworten) installiert, welche danach gar nicht oder nur ungenügend überprüft und angepasst werden. Fast zu jeder verfügbaren Applikation kann man im Internet entsprechende Informationen nachlesen. Diese Online-Datenbanken enthalten die Standard-Benutzernamen und Passworte für alle möglichen Software-Pakete welche auf dem Markt sind.

### 2.1.4 Web-Applikationen und -Auftritte

Viele Lehranstalten bieten inzwischen einen Webauftritt mit Informationen für Schüler, Eltern und Lehrpersonal. Auch die Webserver haben eine schnelle Wandlung mitgemacht. Von der Darstellung einfacher statischer Seiten ausgehend, haben sich die Technologien rasant weiter entwickelt. Es sind nun dynamische Webseiten möglich, wo der Inhalt nach Bedarf zusammengestellt wird. Diese Erweiterung der Webserver-Funktionalität bringt jedoch auch wieder eine Reihe von Sicherheitsproblemen mit sich.

Die Zusammenstellung einer dynamischen Website bedingt, dass ein Benutzer angibt was er will und dies dann vom Server verarbeitet und das Ergebnis dem Benutzer präsentiert wird. Was passiert jedoch wenn man etwas eingibt was der Webserver nicht erwartet? Ein kleines Beispiel wäre folgende URL, welche in die Adresszeile des Browsers eingegeben werden kann:

```
http://www.meineseite.ch/cgi-bin/php?etc/passwd
```

Wenn nun der Zielsever auf Unix/Linux läuft und PHP (im CGI Mode) verfügbar ist, würde obiges Kommando die Unix Passwortdatei auf dem Bildschirm ausgeben, falls das Serversystem nicht ordnungsgemäss konfiguriert ist.

Neben diesem Beispiel, wo eine konzeptionelle Schwäche von CGI (Common Gateway Interface) basierten Applikationen ausgenutzt wird, ist auch der programmierte Code selbst ein potentiell Sicherheitsproblem. Es gibt unzählige Möglichkeiten, Fehler in Programmcode für einen Systemeinbruch auszunutzen.

### 3 Sicherheits-Ratschläge / Grundschutz

#### 3.1 Grundwissen

Um eine Technologie richtig nutzen zu können muss man diese mindestens grundlegend verstehen. Vor allem im schulischen Umfeld, wo der Lehrauftrag im Vordergrund steht, werden die Belange der IT-Sicherheit oft vernachlässigt. Dies ist zu bedauern, da gerade hier junge Menschen mit den sachgemässen (und gesetzeskonformen) Umgang mit Computer und Internet erlernen sollen.

Die Vermittlung von Wissen im Bereich der IT-Sicherheit an Schulen soll vor allem Folgendes erreichen:

##### **Für Lehrkräfte**

- Schaffen von Bewusstsein für die Problematik der IT-Sicherheit
- Aufbau des nötigen Grundwissens für den Schutz der PC-Systeme am Lehrinstitut
- Sensibilisierung der Schüler für Recht und Unrecht in der schwer fassbaren virtuellen Welt
- Lehrkräfte können Schüler und Eltern sensibilisieren für die möglichen Gefahren des Internet (IT-Sicherheit aber auch ungeeignete Inhalte und gefährliche Online-Kontakte zu Erwachsenen)
- Möglichkeit den Kindern und Jugendlichen den Nutzen des PC und Internet aufzuzeigen
- Aufzeigen der Möglichkeiten wie Kinder und Jugendliche ihre Privatsphäre im Internet schützen können

##### **Für Eltern**

- Eltern sollen einschätzen können was Ihre Kinder auf dem heimischen PC machen, was rechtens und was gesetzeswidrig ist
- Eltern sollen befähigt werden, PCs kindertauglich einzurichten (Schutz der Schüler soll nicht an der Schulpforte aufhören)
- Schaffen von Bewusstsein für die Problematik der IT-Sicherheit

##### **Für Schüler**

- Näherbringen der Technologie
- Schaffen von Bewusstsein für die Problematik der IT-Sicherheit
- Vermitteln von "Netiquette" und Online-Verhaltensregeln
- Schaffen von Bewusstsein für Recht und Unrecht mit den neuen Medien
- Vermitteln von Nutzen und Gefahren von PC's und Internet

#### 3.2 Konfiguration

In Bezug auf die IT-Sicherheit ist eine saubere Konfiguration einer Informatik-Komponente, sei dies nun ein Netzwerk-Switch, ein Access Point für Wireless LAN oder ein PC, schon der halbe Weg zu einem sicheren System. Es gibt beim Aufbau und bei der Wartung einer Computer-Infrastruktur einige Grundregeln, welche helfen können:

- **Nichts installieren was nicht benötigt wird**

Viele Applikationen, welche auf dem Markt erhältlich sind bieten sehr viele Optionen welche ein Benutzer fast oder gar nie benötigt. Für ein sicheres System gilt der Grundsatz, nichts zu installieren was nicht benötigt wird. Je

kleiner und übersichtlicher die installierte Basis ist, desto einfacher ist diese zu schützen und desto weniger Angriffsfläche bietet diese für einen Angreifer.

Schauen Sie sich die Optionen, welche Sie bei der Installation eines Programmes haben genau an. Ziehen Sie im Zweifelsfall die "Benutzerdefinierte Installation" einer vom Hersteller vorgegebenen "Standardinstallation" vor und wählen Sie nur aus was Sie benötigen.

- **Prinzip des "So viel wie nötig, so wenig wie möglich"**

Bei der Vergabe von Benutzer- und Systemrechten sollte nur das an Rechten vergeben werden was auch benötigt wird. Wichtig ist hier, auch Berechtigungen zu überprüfen, welche nicht offensichtlich sind (z.B. die Systemfreigaben auf Windows Systemen).

Ein Fehler der oft gemacht wird ist, Konfigurationsproblemen mit der großzügigen Vergabe von Rechten beizukommen. Man sieht oft Schulinstallationen wo jeder Schüler administrative Rechte hat, was sicherlich nicht im Sinne des Erfinders (und des Lehrers) ist.

- **Standardeinstellungen ändern**

Standards sind nicht nur der Freund des Benutzers, sondern auch der des Hackers. Die meisten Applikationen werden mit Standardeinstellungen ausgeliefert, welche für den Benutzer die optimale Nutzbarkeit aber nicht die optimale Sicherheit bietet. Standardeinstellungen müssen überprüft und gegebenenfalls angepasst werden.

Vor allem vom Hersteller vorgegebene Standardpassworte müssen sofort nach der Installation eines Systems geändert werden.

- **RTFM**

Bitte lesen Sie die Handbücher Ihrer Systeme – mindestens den Teil zum Thema Sicherheit. Handbücher von Computern und Software fristen oft ein einsames Dasein im Regal oder wandern schon bei der Lieferung in den Papierkorb. Ich verstehe jeden der nicht gerne Handbücher liest, es kann jedoch massgeblich zur Sicherheit Ihrer Systeme beitragen. In fast allen Fällen enthalten die Dokumentationen ein Kapitel über Sicherheitsfunktionen und -einstellungen. Nutzen Sie diese Informationen.

### 3.3 Härten der Systeme

Das "Härten" der Computer im Schulbetrieb kann bereits wesentlich zur Erhöhung der Sicherheit beitragen. Die nachfolgenden Kapitel sollen, pro Systemwelt, kurz aufzeigen was die wichtigsten Schritte für ein grundlegendes Hardening sind. Aus Platzgründen kann hier nur auf die wichtigsten Punkte eingegangen werden. Die gelisteten Internet-Links verweisen jeweils auf weiterführende Informationen.

#### 3.3.1 Basishärten von Windows Systemen

Das härten von Windows Systemen ist, aufgrund der unzähligen Schwachstellen welche in der Vergangenheit und Gegenwart aufgetreten sind, kein leichtes Unterfangen. Nachfolgend wird nur ein Überblick dargestellt. Einige Links verweisen

für interessierte Windows-Administrationen auf gute Informationsquellen zum Thema.

Zur Einstimmung soll nachstehend kurz gelistet werden welche Microsoft-Tools in Moment die Top 10 Schwachstellen nach Meinung des FBI und des SANS-Institutes darstellen:

1. Internet Information Services (IIS)
2. Microsoft SQL Server (MSSQL)
3. Die Windows Systemauthentifizierung
4. Internet Explorer
5. Windows RAS (Remote Access Services, Fernzugriff, meist mit Modems)
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host (WSH)
8. Microsoft Outlook / Outlook Express
9. Windows Peer to Peer File Sharing (P2P)
10. Microsoft SNMP (Simple Network Management Protocol)

Die Liste zeigt bereits deutlich eines der grössten Probleme, welche zu einem Grossteil für die permanent aufkommenden Schwachstellen bei Windows Systemen verantwortlich sind: die tiefe Integration der Microsoft Applikationen und Services mit dem Betriebssystem.

Nachstehend soll auf das aktuellen Client-Betriebssystem der Windows-Reihe kurz eingegangen werden. Die Server-Versionen von Windows würden den Rahmen dieses Artikels sprengen.

Links zum Thema: <http://www.sans.org/top20/top20-v40-german.pdf>

#### 3.3.1.1 Allgemeines – Patch Management

Einer der wichtigsten Punkte bei der Sicherung von Windows-Systemen ist das Patch-Management. Nachdem in den letzten Monaten etwas Ruhe eingekehrt ist, werden nun wieder fast auf täglicher Basis neue Sicherheits-Updates zur Verfügung gestellt. Während sich die Updates für nicht kritische Einzelgeräte relativ gut automatisieren lassen, muss man für die Server und Computerzimmer etwas mehr Aufwand betreiben.

##### **Updates und Patches automatisieren**

Für das Patch-Management in Schulen bieten sich die "Software Update Services" von Microsoft an. Das Tool ist kostenlos bei Microsoft erhältlich und kann als zentrales Update- und Patch Management System betrachtet werden. Der Vorteil hier ist vor allem in der zentralen Konfigurationsmöglichkeit zu sehen und der eingesparten Bandbreite – die Patches müssen nicht mehr für jedes System vom Internet heruntergeladen werden sondern nur einmal. Die Verteilung auf die Rechner im Computerzimmer erfolgt dann über das interne Netzwerk. Es lässt sich ausserdem festlegen, welche Sprachen und Windows-Versionen man überhaupt in Betracht ziehen will.

Eines ist jedoch eminent wichtig: Erst Testen, dann installieren. Es kommt immer wieder vor, dass sich Fehler in Sicherheits-Updates oder Service-Packs einschleichen, welche dann mehr Schaden verursachen als der Virus vor dem Sie hätten schützen sollen. Es empfiehlt sich hier, auf einem nicht-kritischen System zu testen, und dann erst in die Breite auszurollen.

Links zum Thema:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C>

### **Feststellen des Status Quo**

Microsoft bietet für die Analyse des Sicherheits- respektive Patch-Status von Windows Systemen einige nützliche Tools an. Einerseits ist dies der MSBA (Microsoft Baseline Security Analyzer) und andererseits das "Office Update Inventory Tool". Der MSBA kann ein einzelnes System oder eine Reihe von Systemen in einer Domäne auf übliche Fehlkonfigurationen und fehlende Sicherheits-Patches hin untersuchen. Das Tool bietet eine graphische Oberfläche, ist aber auch in einer Kommandozeilen-Version verfügbar (für Hardcore-Admins). Rein für das Office Umfeld bietet sich das "Office Update Inventory Tool" an, welches einzelne Systeme oder ganze Netzwerke auf den Update-Status der installierten Office-Pakete hin untersucht. Das Tool zeigt an was installiert und was an neuen Updates verfügbar ist.

Links zum Thema:

<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>  
<http://www.microsoft.com/office/ork/2003/journ/offutoolv2.htm>

### **3.3.1.2 Windows XP Professional**

#### **Filesystem Sicherheit**

Windows XP bietet nach wie vor die Möglichkeit, Laufwerke mit zwei Arten von Dateisystemen zu formatieren: FAT32 und NTFS. Aus Sicht der Sicherheit sollte in jeden Fall NTFS verwendet werden, da dieses massiv bessere Sicherheitsfunktionen bietet. Ein Wehmutstropfen bleibt: Wenn Sie beispielsweise Linux parallel auf einem Windows XP System mit NTFS Festplatten betreiben, können Sie von Linux aus nicht so einfach schreibend auf die NTFS Partition zugreifen.

So prüfen Sie, welches Filesystem Sie verwenden:

1. Einloggen mit administrativen Rechten
2. Doppelklick auf "Mein Computer"
3. Rechts-Klick auf das zu untersuchende Laufwerk
4. Anwählen von "Eigenschaften"
5. Die erste angezeigte Seite zeigt das Dateisystem an (z.B. "Dateisystem: NTFS")

Falls Sie noch FAT oder FAT32 Partitionen verwenden können Sie diese wie folgt konvertieren:

1. Anwählen von "Start" und "Ausführen"
2. Eingeben von "cmd" und OK klicken
3. Im Shell-Fenster folgendes eingeben: `convert c: /FS:NTFS /V` (als Beispiel für das c: Laufwerk)
4. Enter-Taste drücken
5. Für alle zu konvertierenden Laufwerke wiederholen
6. Reboot des Systems

Achtung: Bei solchen Aktivitäten sollte immer zuerst ein Backup des Systems erstellt werden.

### **Abschalten von automatischen Logins**

Kein System im Schulbetrieb sollte auf automatische Logins eingestellt sein. Einerseits aus Sicherheitsgründen und andererseits um die Lernenden gleich die Nutzung von Sicherheitsmechanismen nahe zu legen.

Falls automatische Logins verwendet werden, können diese wie folgt beschrieben deaktiviert werden:

1. Auswählen von "Start → Performance and Maintenance → Administrative Tools → Local Security Policy
2. oder für "Classic View": "Start → Settings → Control Panel → User Accounts
3. Nun ist sicher zu stellen das alle lokalen Benutzer mit einem Passwort ausgestattet sind

Sobald ein Benutzerkonto ein Passwort gesetzt hat, ist ein automatischer Login damit nicht mehr möglich.

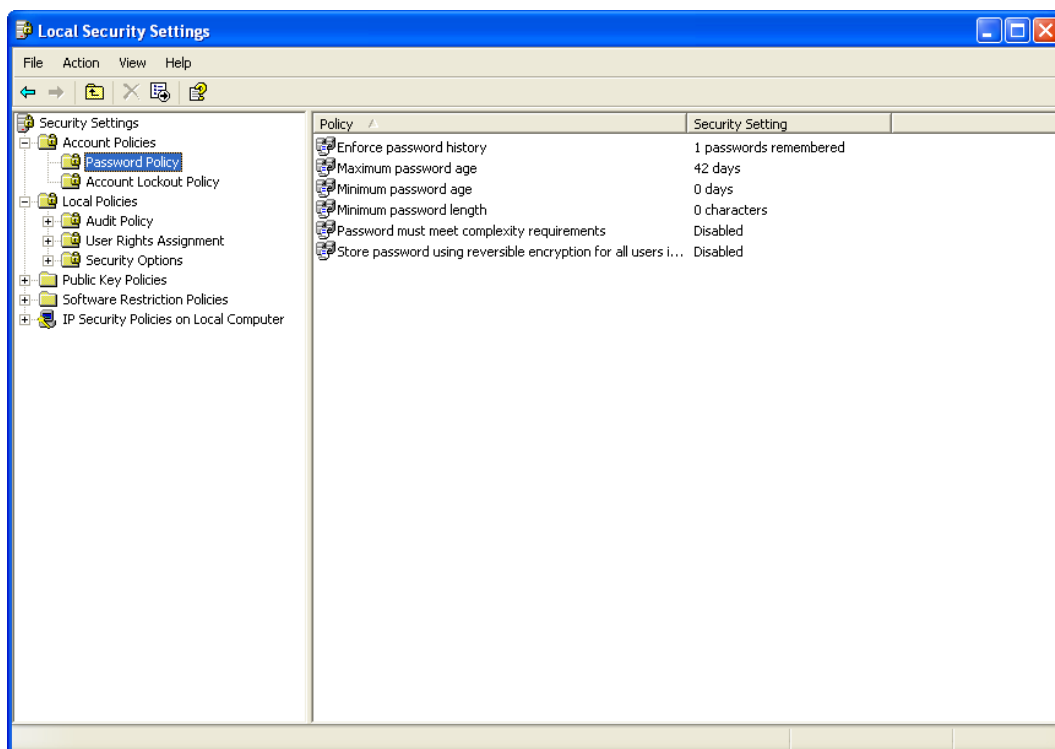
### Lokale Security Policies

Dieser Abschnitt beschreibt die möglichen Sicherheitseinstellungen, welche in den Lokalen Sicherheitsrichtlinien getroffen werden können. Falls Ihr System in einer Windows Domäne (mit Active Directory) integriert ist, können die gelisteten Einstellungen auch in einen "Group Policy Object" (GPO) gespeichert werden. Die Nutzung von einer Domäne und deren Sicherheitsfunktionen ermöglicht eine zentrale Verwaltung von Sicherheitsrichtlinien für alle angeschlossenen Windows-Systeme. Die Handhabung der Sicherheitsrichtlinien lokal oder in einer Domäne sind sehr ähnlich.

Zugriff auf das "Local Security Policy Editor Tool" erhalten Sie wie folgt:

1. Auswählen von "Start → Performance and Maintenance → Administrative Tools → Local Security Policy
2. oder für "Classic View": "Start → Settings → Control Panel → Administrative Tools → Local Security Policy"

Das Local Security Policy Editor Tool erlaubt eine Vielzahl von Einstellungen in Bezug auf die Sicherheit des lokalen Systems. Es empfiehlt sich, die Möglichkeiten der Policy genau zu studieren.



Mindestens die "Password Policy" und die "Account Lockout Policy" sollten entsprechend eingestellt werden.

Ein kleines Wort der Warnung: Es kann passieren, dass man sich – auch als Administrator – selbst komplett aus dem System aussperrt. Im Zweifelsfall also besser Nachlesen oder –fragen.

### Default Benutzerkonten

Im Standard wird ein Windows XP System mit einem Administrator und einem Gast Konto ausgestattet. Da jeder weiss wie diese Benutzerkonten heissen, ist es ratsam, diese umzubenennen. Noch wichtiger ist es allerdings, für das Administrator, wie auch für das Gast-Konto starke Passworte zu verwenden. Es wird empfohlen, ein starkes Passwort für das Gast-Konto zu setzen und dieses dann wieder zu deaktivieren.

Leider lässt Windows XP nicht zu dass man das Gast-Konto gleich ganz löscht. Auf jeden Fall sollte das Konto deaktiviert bleiben (siehe Abschnitt "Dateizugriff und Freigaben").

### Dateizugriffe und Freigaben

Wenn man die Rechtevergabe bei Freigaben betrachtet, macht Windows XP keinen guten Job in Punkto Sicherheit. Wird nämlich ein neuer Share (beispielsweise auf das Stammverzeichnis des C-Laufwerkes "C:\") erstellt, erhält die Gruppe "Everyone" vollen Zugriff darauf. Ist nun das Gast-Konto aktiviert, hat auch dieses (als Mitglied der Everyone-Gruppe) vollen Zugriff. Nicht sehr vorteilhaft aus Sicht der Sicherheit.

Bei der Verwendung von Freigaben muss unbedingt darauf geachtet werden, dass eine klare Zugriffsregelung besteht. In den seltensten Fällen sollte der Gruppe "Everyone" überhaupt Zugriff auf einen Share gegeben werden. Hier gilt wiederum der Grundsatz "So viel wie nötig – so wenig wie möglich".

Eine Spezialität von Windows sind die so genannten "System Shares". Windows legt für jedes der im System vorhandenen Partitionen (z.B. C:, D: oder E: für ein CD-ROM) einen "System Share" an. Diese Freigaben können aber auch von Benutzern verwendet werden, und zwar wie folgt:

1. Klick auf "Start → Ausführen"
2. Eingeben von "cmd" und Enter-Taste drücken
3. Geben Sie "\\Ihr\_computername\c\$" ein und drücken Sie die Eingabetaste

Dies funktioniert natürlich auch über das Netzwerk. Ersetzen Sie einfach "Ihr\_computername" durch den Namen eines Rechners im Netzwerk und Sie können auf das Laufwerk zugreifen. Je nachdem wie die Rechte des Zielsystems eingestellt sind, erfolgt nicht einmal mehr eine Passwortabfrage.

### 3.3.2 Basishärten von Macintosh Systemen

#### Up-to-date bleiben

Eine einfache Art, wichtige Fehlerkorrekturen und Sicherheitspatches möglichst bald nach Erscheinen zu erhalten. OS X bietet über die Funktion "Software Update" die Möglichkeit den Vorgang zu automatisieren. Standardmässig wird "Software Update" wöchentlich automatisch gestartet, dieser Wert sollte bei exponierten Systemen jedoch auf einen kürzeren Zeitraum (Täglich) gesetzt werden:

1. Click auf "System Preferences" → "Software Update " (Tab)
2. Ändern des Defaultwertes von "Wöchentlich" auf "Täglich"
3. Verlassen der "System Preferences"

Achtung: Obwohl Apple sicher eine der besseren Qualitätssicherungs-Prozesse in der Software-Industrie hat, können sich in solche Patches Fehler einschleichen. Daher bitte immer erst – sofern möglich – auf einem nicht-kritischen System testen.

#### **Abschalten unnötiger Services**

Mac OS X hat in der Default-Installation alle Services die auf dem "inetd" (dem Internet Master-Dienstprozess) laufen abgeschaltet. Falls Sie nicht sicher sind, können Sie diese Einstellungen in `/etc/inetd.conf` überprüfen, z.B. mit einem Texteditor oder dem Shell-Kommando `cat /etc/inetd.conf`.

Betreffs dieser Default-Einstellung gibt es unter Umständen eine Ausnahme: Den FTP-Service kann man auch über die System Preferences einstellen (System Preferences → Sharing → File & Web). Hier kann die Checkbox "Allow ftp access" an- oder abgewählt werden.

Falsch konfigurierte Services können grosse Sicherheitslücken im System hinterlassen, daher sollte grossen Wert auf eine richtige Konfiguration nach dem "so wenig als möglich – so viel wie nötig" Prinzip gelegt werden. Wenn ein Service läuft und Sie wissen eigentlich gar nicht so richtig was er macht – schalten Sie ihn ab. Wenn er wichtig war wird sich jemand melden, wenn nicht, hat man ein potentielles Sicherheitsleck gestopft.

Falls es auf einem Ihrer Systeme nötig ist, Internet-Services anzubieten, beispielsweise für Webserver, FTP-Server oder ähnliches, bietet sich der Einsatz von so genannten "TCP Wrappers" an. Diese arbeiten als "Mittelsmann" zwischen der Aussenwelt und den System-Services und bieten eine massiv bessere Kontrolle über diese als das ohne Wrappers möglich wäre. So können Anfragen gefiltert werden um beispielsweise ein "Spoofing" (siehe Glossar) oder eine "TCP Sequence prediction" (siehe Glossar) zu verhindern. Bei OS X ist bereits ein Open Source Produkt integriert, welches genau diese Aufgaben erfüllt: "TCPWrappers".

Links zum Thema: <http://www.hmug.org/HowTos/tcpwrappers.html>

#### **Sichere Fernwartung**

Unix-Basierte Systeme bieten oft eine Reihe von Standard-Services die äusserst unsicher sind, wie beispielsweise Telnet, FTP, Rlogin und einige weitere. Vor allem für administrative Tätigkeiten sollte man auf Protokolle setzen welche eine stärkere Authentisierung und eine Verschlüsselung der Kommunikation bieten.

Mac OS X bietet von Haus aus Unterstützung für SSH (OpenSSH wird mitgeliefert). SSH (Secure Shell) ist ein Protokoll, welches sich hervorragend eignet für die System Fernwartung

Links zum Thema: [www.openssh.org](http://www.openssh.org)  
[www.ssh.com](http://www.ssh.com)

#### **Personal Firewall**

Der Einsatz von Personal-Firewall Software ist generell auf jedem System zu empfehlen. Die Personal Firewall von Mac OS X bietet die Möglichkeit, allen eingehenden Netzwerkverkehr zu prüfen. Erlaubte Verbindungen werden durch gelassen, alle anderen nicht. Die Mac OS X Personal Firewall basiert auf "ipfw", einer Technologie, welche sich schon seit einigen Jahren auf Unix Systemen bewährt hat. Das Management der Personal Firewall ist im "Sharing" Tab integriert und erlaubt die einfache Konfiguration über das anwählen von Checkboxes zu vordefinierten Services (wie beispielsweise IRC). Natürlich ist es auch möglich, neue Services selbst zu definieren. Zugriff auf die Firewall erhalten Sie wie folgt:

1. Öffnen der "System Preferences" → Sharing → Firewall

2. Auf "Start" klicken
3. "System Preferences" wieder verlassen

Wem die Funktionalität der integrierten Firewall nicht ausreicht, sollte sich eines der kommerziellen Drittprodukte näher ansehen.

Links zum Thema: <http://www.roadstead.com/weblog/Tutorials/firewall.html>  
[http://www.symantec.com/sabu/nis/npf\\_mac/](http://www.symantec.com/sabu/nis/npf_mac/)

### Benutzersicherheit

Obwohl Mac OS X bereits "ab Fabrik" mit relativ guten Sicherheitseinstellungen zum Thema Benutzer ausgeliefert wird, gibt es doch einige Einstellungen welche angepasst werden sollten.

#### Root Benutzer

Mac OS X hat bei Auslieferung den "Root" Account deaktiviert, jedoch hat dieser ein leeres Passwort. Bei einer Kompromittierung eines solchen Systems ist es für den Angreifer sehr einfach, volle Kontrolle über das System zu erlangen.

Zum setzen eines Root Passwortes muss folgende Prozedur durchgeführt werden:

1. Klick auf den Finder
2. Auswählen von "Go → Applications"
3. Öffnen von "Utilities"
4. Öffnen von "Netinfo Manager"
5. eingeben eines Benutzernamen und Passwortes eines Administrativen Nutzers
6. Auswählen von "Security → Enable Root User"
7. Beim ersten Setzen des Root Passwortes erscheint ein "Netinfo Error", der anzeigt dass das Passwort leer ist
8. Geben Sie ein Root Passwort ein (siehe Link zu den Richtlinien für sichere Passworte) und klicken Sie auf "Set"
9. Nochmals das Passwort eingeben und auf "Verify" klicken
10. Auswählen von "Security → Disable Root User"

#### Richtlinien für sichere Passworte

Obwohl es schon einige alternative Technologien zur Authentisierung gibt, ist die Kombination von Benutzername und Passwort immer noch die am meisten gebrauchte Methode. Der Mensch neigt zur Bequemlichkeit und wählt Passworte, welche er sich einfach merken kann – wie beispielsweise die präferenzierte Feriendestination, der Name des Hundes oder die Telefonnummer. Aus heutiger Sicht sind alle diese Passworte schwach und durch ein modernes Hackertool in-ner Sekunden oder Minuten zu knacken.

Es gibt Tricks und Tipps wie man sich ein sicheres Passwort ausdenken und sich auch merken kann. Das nachfolgend verlinkte Dokument gibt wertvolle Tips:

Links zum Thema: <http://www.digital-freedom.net> (Tools → Password Auditing)

### Sonstige Einstellungen

Auto Logon

Bei einer Default-Installation ist Mac OS X so konfiguriert, dass ein Autologon stattfindet mit dem administrativen Benutzer der zuerst im System erfasst wurde. Zusätzlich zeigt OS X alle validen Benutzerkonten im Login-Fenster und präsentiert nach drei erfolglosen Versuchen einen Passwort "Hinweis". Alle diese Funktionen sind zwar bequem für den Benutzer – helfen aber auch dem Angreifer, und sollten daher abgeschaltet werden. Folgende Prozedur beschreibt die Sicherung des Login Vorganges:

1. Öffnen der "System Preferences → Accounts → User"
2. Abwählen der Option "Log in automatically as..."
3. Klicken auf "Login Options"
4. Setzen von "Display Login Window as..." auf "Name and Password"
5. Abwählen der "Show password hint after 3 attempts..." Option

#### Screen Saver Passwort

In einem Raum wo sich mehrere Personen aufhalten, sollte das System jeweils "geloockt" werden wenn man den Raum verlässt. Um der Vergesslichkeit vorzubeugen kann man auch den Bildschirm-Schoner mit Passwortschutz aktivieren:

1. Klick auf "System Preferences → Screen Effects → Activation"
2. Setzen von "Time until screen effect starts" = 5 Minuten
3. Setzen von "Password to use when waking the screen effect" = "use my user account password"
4. Klicken auf "Hot Corners" und setzen einer Bildschirm-Ecke für die schnelle Aktivierung des Bildschirmschoners

#### Open Firmware Passwort

Seit Version 10.1 unterstützt Mac OS X das so genannte "Open Firmware Password". Diese Funktion sollte für kritische Systeme verwendet werden und gegebenenfalls auch für Notebooks. Ein Open Firmware Passwort bringt folgendes:

- Bei gesetztem Passwort kann nur noch von der Harddisk gebootet werden, welche als "Startup Disk" in den "System Preferences" angegeben wurde. Ein booten von CD-ROM, FireWire Disk oder einer anderen Partition, respektive einer anderen Festplatte ist nicht mehr möglich
- Das Open Firmware Passwort ist ausserdem durch die Technik der progressiven Verzögerung gut gegen "Brute-Force" Attacken gerüstet

Um die "Open Firmware Password" Funktion zu aktivieren muss zunächst die Software von Apple heruntergeladen werden (siehe ersten Link unten). Bitte unbedingt zuerst den Artikel über Open Firmware Password (zweiter Link unten) durchlesen. Die Konfiguration erfolgt wie nachfolgend beschrieben:

1. Herunterladen der "Open Firmware Password" Applikation
2. Starten des Programmes
3. Klick auf das Schloss. Und Login mit einem administrativen Benutzer.
4. Klick auf "Change"
5. Anwählen der Checkbox "Require password to change Open Firmware settings"
6. Eingabe eines sicheren "Open Firmware" Passwortes (nicht vergessen!)
7. Klick auf "OK"
8. Nochmaligen Klick auf das "Schloss" um weitere Änderungen an den Einstellungen zu verhindern

### 9. Applikation mit "Quit" verlassen

Links zum Thema: <http://docs.info.apple.com/article.html?artnum=120095>  
<http://docs.info.apple.com/article.html?artnum=106482>

## 4 Linksammlung & Toolübersicht

Es gibt eine fast unüberschaubare Menge von nützlichen und weniger nützlichen Tools zum Thema Sicherheit. Die "DigitalFreedom" (DF) Website soll Administratoren Sicherheits-Profis und interessierten Laien die Auswahl von guten Sicherheits-Tools erleichtern. Die Website bietet eine kategorisierte Übersicht über eine Vielzahl von Tools und wird in regelmässigen Abständen auf den neusten Stand gebracht.

Des Weiteren wird auch eine umfassende Linksammlung und, erstmals auf dem Internet, eine komplette Übersicht über alle verfügbaren RSS-Feeds zum Thema Sicherheit geboten – in Deutsch und Englisch.

Unsere "Virus Watch" Seite zeigt zudem zusammengefasst die neusten Meldungen der wichtigsten Hersteller und Virenjäger zum Thema Viren, Worms und Trojaner.

[www.digital-freedom.net](http://www.digital-freedom.net)

### 4.1 Allgemeine Links zu Mac OS X Sicherheit

Eine gute allgemeine Einführung zu Mac OS X Sicherheit:  
<http://developer.apple.com/internet/security/securityintro.html>

Apple Security Updates  
<http://docs.info.apple.com/article.html?artnum=61798>

Schutz des Dateisystems in der Classic Umgebung  
<http://docs.info.apple.com/article.html?artnum=25422/>

Darwin Security  
<http://www.stosdarwin.org/>

Einführung in die Sicherheit von OS X  
<http://developer.apple.com/internet/security/securityintro.html>

Infos zu Sicherheit des OS X  
<http://www.apple.com/macosx/features/security/>

Mac Sicherheitsportal  
<http://www.macsecurity.org/>

Mac Sicherheitsportal  
<http://www.macintoshsecurity.com/>

SANS Artikel zu Mac Sicherheit

[http://www.sans.org/rr/catindex.php?cat\\_id=34](http://www.sans.org/rr/catindex.php?cat_id=34)

Sicherer Betrieb eines Apache Webservers auf MacOS X

<http://www.macdevcenter.com/pub/ct/49>

### 4.2 Allgemeine Links zu Windows Sicherheit

IIS Lockdown Tool

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DD E9EFC0-BB30-47EB-9A61-FD755D23CDEC>

URLScan Security Tool

<http://www.microsoft.com/downloads/details.aspx?FamilyID=12244f33-a5da-4203-a3a8-83f4388bb71f&DisplayLang=en>

NTBugtraq

NTBugtraq ist eine Mailing Liste zur Diskussion von Sicherheits-Exploits und Bugs in Windows NT, 2000 und XP und weiteren Applikationen.

<http://www.ntbugtraq.com/>

Windows Security Guide

Der Windows Security Guide enthält Informationen und Ressourcen zur Sicherung des Windows Betriebssystems und Details zu den aktuellsten Schwachstellen, deren Behebung, Artikeln und technischem Support.

<http://www.winguides.com/security/>

Microsoft Sicherheits-Portal

<http://www.microsoft.com/germany/ms/security/default.mspx>

### 4.3 Kontakt / Experten-Chat

Fragen und Anregungen zum Thema Sicherheit und zu diesen Seiten nehme ich sehr gerne entgegen. Im Sinne der Weiterentwicklung dieser Seiten bin ich um jede Idee froh, wie diese Seiten erweitert und attraktiviert werden können. Teilen Sie uns mit was Sie weitergehend interessiert.

Bei genügend Interesse sind wir bereit, unsere Experten für Fragen zum Thema "Sicherheit im Bildungswesen" zur Verfügung zu stellen. Dies könnte in der Form eines Experten-Chat oder Forums realisiert werden. Bitte melden Sie sich bei uns falls dies einem Bedarf entspricht.

#### Kontakte:

Themengebiete:	Sicherheit, Educa Dossier, Experten Chat
Ansprechpartner:	Dr. Michael Böni
E-Mail Adresse:	<a href="mailto:mbo@shift-think.com">mbo@shift-think.com</a>

Themengebiete:	Digital Freedom
Ansprechpartner:	Carole Hofmann
E-Mail Adresse:	<a href="mailto:cho@digital-freedom.net">cho@digital-freedom.net</a>

## 5 Themen für die nächsten Erweiterungen des Dossiers

Es ist geplant, das Dossier in regelmässigen Abständen zu erweitern und auf dem neusten Stand zu halten (nichts ist älter als ein Sicherheits-Dossier von gestern). Fehlen Ihnen Themen? Welche Themen hätten Sie gerne vorrangig behandelt? Melden Sie sich bei uns!

Themenliste:

1. **Tool-Grundausstattung:** Welche Sicherheits-Tools sollten mindestens eingesetzt werden
2. **Incident Management:** Wie erkenne ich einen Systemeinbruch
3. **Computer Forensik:** Spuren sichern und dokumentieren
4. **Sicherheit organisieren:** Wie organisiere ich IT-Sicherheit in Schulen
5. **Erste Hilfe:** Konkrete Vorgehensweisen bei konkreten Sicherheitsproblemen (Schritt für Schritt Anleitung und Verwendung von Tools)