



Sicherheit im Schulnetz

AdministratorInnen können schwer abschätzen, welche Sicherheitslücken in ihrer Informatik-Infrastruktur bestehen. Zudem sind sie viel zu beschäftigt oder oft überfordert, alle Lücken zu schliessen.

Hacker wählen die am einfachsten knackbaren Lücken mit Angriffen, für die vorgefertigte Tools existieren oder leicht durchführbar sind.

Im Folgenden stellen wir die für Schulbetriebe grössten Sicherheitsrisiken und mögliche Lösungsansätze zusammen.

Sicherheitsrisiken im Schulbetrieb **Was sind gute Passwörter?**

Passwörter stellen eine wichtige Zugangskontrolle dar. Dennoch verwenden viele – der Einfachheit halber – leicht erratbare Passwörter. Zudem werden viele Systeme ohne oder mit Standard-Passwörtern ausgeliefert, die nach Inbetriebnahme nicht geändert werden.

Lösungsansätze:

- Standardpasswörter nach Installation ändern
- Verwendung «starker» Passwörter:
 - min. 8 Zeichen lang
 - keine Begriffe oder Namen, die naheliegend sind
 - Mischung von Gross-/Kleinbuchstaben, Zahlen und Sonderzeichen
 - Schulung und Sensibilisierung der BenutzerInnen
 - Regelmässiges Ändern der Passwörter

Auch «kryptische» Passwörter können in einer Form sein, die sich ein Benutzer gut merken kann und trotzdem kaum zu knacken sind. Der bekannte Satz «To be or not to be – that is the question» lässt sich zum Beispiel zu einem «guten» Passwort verarbeiten: 2bon2b-tit?

Oft schützt man sich mit Passwörtern vor sich selbst. Passwörter gehen vergessen oder AdministratorInnen sind abwesend. Daher ist es ratsam, zu bestimmen:

- welche Bereiche für alle zugänglich sein müssen
- wo versiegelte/verschlossene Passwort-Couverts aufbewahrt werden (z.B. im Tresor des Schulsekretariats)
- wo alte Passwörter zu finden sind (falls auf ältere Backups zurückgegriffen werden muss).

Nicht existierende oder unvollständige Backups

Wenn Daten gelöscht oder verfälscht wurden, benötigt man ein Backup. Viele Schulen erstellen zwar mehr oder weniger regelmässig Backups, überprüfen aber nie, ob diese auch funktionieren.

Lösungsansätze:

- Erstellen eines Backup-Konzepts
 - Arten und Zeiten des Backups
 - Wiederherstellung der Daten
 - Dokumentation
 - Notfall-Prozeduren
- Regelmässiges Durchspielen des Ernstfalles

Wichtig ist, dass Backups in mehreren Generationen existieren. Oft werden Datenverluste nicht sofort bemerkt und es wird notwendig, auf Versionen der Vorwoche oder des Vormonates zurückzugreifen. Datenträger sind zudem getrennt vom Original aufzubewahren für den Fall, dass es zu Datenverlust infolge Feuer, Wasser, Vandalismus oder Diebstahl kommt.

Fehlende Trennung von Schule und Verwaltung

Die sensibelsten Daten im Schulbetrieb befinden sich in der Verwaltung: vertrauliche Daten zu SchülerInnen, LehrerInnen und Behörden. Wenn das Netz der Schule nicht physisch getrennt ist vom Netz der Verwaltung, besteht ein hohes Risiko, dass aus Unachtsamkeit oder Böswilligkeit nicht berechtigte Benutzer Zugang zu diesen Daten erhalten.

Lösungsansätze:

- Trennung von Schul- und Verwaltungsnetz
- Speicherung auf separaten Datenträgern

Education Team
Service und Support
Hard- und Software
www.ingeno.ch
info@ingeno.ch
www.nettocomputer.ch

Ingeno Computer
Netto Computer
Netto Computer

Netto Computer
Netto Computer
Ingeno Data

8047 Zürich, Fellenbergstrasse 291, 01 406 12 12
8047 Zürich, Fellenbergstrasse 291, 01 406 12 34
8305 Dietlikon, Brandbachstrasse 8, 01 805 75 05

3001 Bern, Nydeggestalden 8, 031 311 23 00
8200 Schaffhausen, Grabenstr. 2, 052 634 08 08
4001 Basel, Güterstrasse 2, 061 366 11 11

Kein Schutz vor Viren, Würmern und Trojanern

Viren & Co. sind vor allem auf Windows-Systemen ein weitverbreitetes Problem, können aber auch Macintosh-Systeme befallen, vor allem E-Mail-Viren in Outlook und Makro-Viren in MS Word und Excel.

Lösungsansätze:

- Virenschutzprogramme mit regelmässigen (monatlichen!) Updates der Virendefinitionen.
- Verwendung alternativer Produkte zu MS Office und Outlook.

Offene Zugänge aus dem Internet

Ist das Schulnetz über ADSL, Kabelmodem oder Standleitung mit dem Internet verbunden, erhöht sich das Risiko, von Hackern attackiert zu werden. An sich ist das Eindringen in ein Schulnetz nicht interessant für Hacker, da damit weder Geld noch «Ehre» zu holen ist. Die Computer einer Schule können aber auch als Relais-Stationen für Angriffe auf andere Computer-Systeme missbraucht werden.

Lösungsansätze:

- Schutz des Netzwerks und Zugriffskontrolle durch eigenen FireWall.

Risiko-Analyse von Ingeno

Die Ingeno erarbeitet das Risiko-Profil Ihrer Schule und schlägt Ihnen Massnahmen zur Reduktion des Risikos vor.

Im Einzelnen beinhaltet diese Grob-Risiko-Analyse:

- Eruiieren der Sicherheitsbedürfnisse und -ziele
- Bestandesaufnahme
- Organisation Netzwerk (physisch und logisch)
- Kritische Daten/Rechner
- Verbindungen nach aussen
- Vorhandener Schutz
- Benutzer- und Passwort-Verwaltung
- Aufzeigen der kritischen Punkte...
... und Empfehlung für Massnahmen zum Erreichen der Sicherheitsziele samt Kostenschätzung.

Preis: Fr. 900.– (Fr. 740.– für SESAM-Kunden)
Mit schriftlicher Dokumentation Fr. 1800.–/Fr. 1480.–

Ingeno-Backup-Konzept

Die Ingeno erstellt in einem Halbtage zusammen mit Ihnen Worst-Case Szenarien, erarbeitet ein Backup-Konzept.

Welches sind Ihre wichtigen Daten?
Wo sind sie gespeichert?
Wieviele Generationen sind notwendig?
Wie prüfe ich Backup-Sets?
Wie lange darf das Wiederherstellen von Daten dauern?
Wo lagere ich Speicher-Medien?

Preis Fr. 900.– (Fr. 740.– für SESAM-Kunden)
Inkl. schriftlichem Konzept.

Intensiv-Workshop “MacManager”

**Effiziente Computerverwaltung in der Schule
2 Halbtage**

Kurs 1: 19./26. Juni ausgebucht

**Kurs 2: Samstag, 14. und 21. September 2002,
jeweils 9.00–12.00 Uhr
Pestalozzianum Zürich, Kursraum 2**

MacManager ist das Werkzeug von Apple zur einfachen und leistungsfähigen Administration von Netzwerken.



MacManager schützt die Arbeitsstationen und bietet dem Benutzer immer die gleiche Arbeitsumgebung mit eigenen Dokumenten und Präferenzen auf jeder Arbeitsstation des Netzwerks. Der Administrator importiert die Benutzer in eine übersichtliche und einfach zu bedienende

Applikation. Den Gruppen und Benutzern werden Profile zugeteilt (erlaubte Programme, Druckerzugriff, Serverzugriff, Interneteinstellungen usw). Dank MacManager haben Sie Ihr Netzwerk besser im Griff und sparen Zeit und Geld.

Dieser Workshop ist für Informatikverantwortliche und interessierte Lehrkräfte gedacht. Als Server verwenden wir MacOS X Server 10.1 und Macintosh Management Server 2.1 – als Client MacOS 9.x.

Themen:

- Mögliche Konzepte der Zugriffsregelung
- Einrichtung und Import von Benutzern aus verschiedenen Quellen (AppleShareIP, Filemaker-Datenbank, Excel-Tabelle)
- Definition von Benutzer- und Gruppenrechten
- Programm-, Drucker- und Speicherplatz-Verwaltung
- Besonderheiten bei der Installation von Anwender-Programmen unter Macintosh Manager
- Verwaltung von Programm- und System-Voreinstellungen
- Erstellen von Reports zu Benutzeraktivitäten, Programmverwendungen, Druckseiten- und Speicherplatz-Zuteilungen
- Troubleshooting

Die Beschränkung auf 12 TeilnehmerInnen garantiert einen optimalen Kurserfolg.

Preis: Fr. 390.– inkl. Kursunterlagen.

Anmeldung für den Septemberkurs mit beiliegender Antwortkarte oder per E-Mail an <a.oettli@ingeno.ch> bis spätestens 15. Juli 2002. Für Fragen wenden Sie sich direkt an Andreas Oettli, Tel. 01 406 12 12.