KANTON LUZERN

Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt Schulen ans Internet

1. Zweck des Merkblattes

An immer mehr Schulen nutzen Lehrer und Schüler das Internet. Die Möglichkeiten sind vielfältig und werden je länger je mehr effektiv genutzt. Dieses Merkblatt soll aufzeigen, welche Gefahren durch die vermehrte Nutzung des Internets für die Schulen entstehen und wie ihnen entgegengetreten werden kann.

2. Datenschutz im Internet

Bei jeder Aktivität im Internet, ob beim Schreiben eines eMails, beim Besuch einer Website, beim Ausfüllen eines Online-Formulars oder beim Eintrag in einer News-Group, hinterlässt ein Anwender Datenspuren. Mit Hilfe von Cookies[1] werden diese Daten gezielt gesammelt, miteinander kombiniert und schlussendlich nicht selten zu einem Persönlichkeitsprofil zusammengefasst. Auch die schuleigene Homepage kann in diesem Fall zum Aufbauen von Persönlichkeitsprofilen beitragen.

Erstellte Persönlichkeitsprofile können zum Verkauf angeboten und für gezielte Marketingmassnahmen oder für Abklärungen über eine Person (z.B. vor einer Anstellung) verwendet werden. Da diese Anbieter sehr häufig aus dem Ausland ihre Dienste anbieten, ist ein Löschungsanspruch meist nicht durchsetzbar.

Neben dieser unkontrollierbaren Verbreitung von Daten über den Anwender entstehen durch den Einsatz des Internets an den Schulen noch weitere Gefahren:

3. Gefahren durch die Nutzung des Internets an Schulen

- *Gefahr durch Virenangriffe*
  Eine grosse Gefahr droht durch Viren, Trojanische Pferde und andere schädliche Programme, die bei der Nutzung des Internets oder der eMail-Dienste auf die Schulinfrastruktur gelangen können. Dies kann zu Ausfällen von Hard- und Software, zu Datenverlusten oder zum Missbrauch von sensitiven Daten führen und kann entsprechend weitreichende Folgen haben.

[1] Kleine Dateien welche Nutzerdaten speichern und diese an den Betreiber der Internetseite zurückliefert.

- *Unsichere Kommunikation*
  Grundsätzlich ist der Versand von eMails ohne Verschlüsselung nicht sicher. Das Versenden von eMail wird häufig mit dem Versenden einer Postkarte verglichen. Sie kann von jeder und jedem eingesehen werden. Aus diesem Grund dürfen keine sensitiven Daten über das eMail versandt werden.
  Eine weitere Problematik in der Kommunikation im Internet ist die mangelnde Authentizität. Es kann nicht mit Bestimmtheit festgestellt werden, ob unser Kommunikationspartner wirklich die Person ist, für welche er sich ausgibt und ob die erhaltenen Information wirklich die Daten sind, welche von "unserem" Absender versandt wurden. Es fehlt demnach noch an einer genügenden elektronischen Signatur.

- *Mögliche Rufschädigung*
  Für die Schule, aber auch für unbeteiligte Nutzer, kann eine Rufschädigung entstehen, wenn rechtswidrige Inhalte wie Rassismus, Gewalt, Pornographie oder Terrorismus über die Schulinfrastruktur aufgerufen oder verbreitet werden. Das selbe gilt für strafbare Aktionen, wie beispielsweise das Lancieren eines Virus über das Schulnetz.

- *SPAM Attacken*
  Wenn zu viele Datenspuren hinterlassen und die schuleigenen eMail-Adressen nicht umsichtig eingesetzt werden, steigt die Gefahr von unerwünschten SPAM Attacken. Dabei handelt es sich um ungewünschte, meist zwielichtige Werbemails.

4. Technische Massnahmen

Die Umsetzung der nachfolgenden Schutzmassnahmen sind dringend empfohlen:

- *Zugriffschutz auf Computern*
  Grundsätzlich sollen alle Computer im Schulnetzwerk so geschützt werden, dass sich ein Anwender vor der Nutzung mit einem Passwort anmelden muss. Passwörter dürfen aber niemals auf dem Computer gespeichert oder hinterlegt werden.

- *Sichere Einstellungen für die Software*
  Browser und eMail-Programme müssen sicher konfiguriert, die neusten Updates installiert und die Sicherheitseinstellungen auf die grösstmögliche Stufe eingestellt werden. Zusätzlich sollte das Ausführen von Makros in den Microsoft Standard Produkten nicht erlaubt sein.

- *Firewall und Virenscanner einsetzen*
  Mit dem Einsatz einer Firewall soll verhindert oder zumindest erschwert werden, dass Unbefugte über das Internet auf Ihren Computer gelangen können. Mit einem Virenschutzprogramm sollen Viren rechtzeitig erkannt und gelöscht werden, bevor sie Schaden anrichten können.

- *Einbau eines SPAM-Filters*
  Mit dem Einsatz eines SPAM-Filters sollen unerwünschte Werbemails abgeblockt werden.

- *Verschlüsselung von Informationen*
  Die Verschlüsselung beim eMail-Verkehr verhindert, dass unbefugte Dritte, die beim Übertragen ihres Mails dieses abfangen, die Daten missbrauchen können. Nur wer die Daten mit dem richtig Key entschlüsselt, kann das eMail effektiv lesen.

- *Löschen von Datenspuren*
  Nach Abschluss der Arbeiten im Internet sollen manuell oder automatisch die hinterlassenen Datenspuren (History, Cookies, Cache) auf dem Computer gelöscht werden.

- *Trennen der Schulverwaltung vom Schüler-Netzwerk*
  Die Daten der Schulverwaltung sollten aus Sicherheitsgründen nicht auf dem selben Netzwerk liegen, mit welchem die Schülerinnen und Schüler arbeiten und über welches sie ins Internet gelangen.

- *Einsetzen von Filterprogrammen*
  Der Einsatz von Filterprogrammen verhindert oder erschwert zumindest den Zugriff auf nicht erwünschte oder unzulässige Internetangebote.

5. Erzieherische Massnahmen

Die oben erwähnten Schutzmassnahmen garantieren alleine noch keine „saubere“ Benutzung des Internets. Die erzieherischen Massnahmen, insbesondere an Schulen, sind im gleichen Rahmen wichtig, wie die technischen Vorkehrungen.

Grundsätzlich ist es von grosser Bedeutung, dass die Schülerinnen und Schüler über die Risiken informiert und für die Problematik sensibilisiert werden. Die Eigenverantwortung muss wahrgenommen werden. Eine 100%-ige Sicherheit wird kaum je erreicht werden können.

Aus diesem Grund sollen verbindliche Regeln aufgestellt und eine Nutzerordnung abgegeben werden, welche folgende Punkte enthalten soll:

- Die Risiken, die mit der Nutzung des Internets verbunden sind;
- Hinweise, wie die Datenspuren im Internet hinterlassen werden;
- Rechte, Pflichten und Verantwortlichkeiten eines Nutzers;
- Hinweise darauf, dass die Aktivitäten im Hintergrund protokolliert werden;
- Lehrpersonen müssen die Schülerinnen und Schüler bei der Nutzung beaufsichtigen;
- Was bei der Nutzung des Internets nicht erlaubt ist und welche Seiten nicht aufgerufen werden dürfen;
- Folgen bei einer Pflichtverletzung.

6. Schlussfolgerung

Der Nutzen des Internets für den Schulbetrieb ist unbestritten. Doch einen 100%-igen Schutz vor allen Gefahren gibt es nicht. Es ist sinnvoll, dass die Schülerinnen und Schüler diese Gefahren kennen und bewusst mit ihnen umzugehen lernen. Die Schule hat diesbezüglich ihre Erziehungsaufgabe wahrzunehmen.

7. Fragen und Informationen

Für Fragen und weitere Informationen zum Internet an Schulen stehen Ihnen die Datenschutzbeauftragten gerne zur Verfügung.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	+ 41 41 228 66 06
Fax:	+ 41 41 228 69 13
eMail:	dsb@lu.ch **WARNUNG**: Der eMail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in eMails!
Internet:	http://www.datenschutz.lu.ch

Luzern, Dezember 2003