

Sicherheit im Internet?!

Autor: Jürgen Rathmayr



Mit Sicherheit wird auch in Ihrer Schulbibliothek gerne im Internet gesurft. – Aber surft man auch mit Sicherheit im Internet? – Klar, man navigiert doch anonym im World Wide Web von Seite zu Seite! – Oder vielleicht doch nicht?

Falls Sie sich einmal ein Bild davon machen wollen, welche Spuren Sie beim vermeintlich anonymen Surfen im Internet hinterlassen, so empfehle ich Ihnen den Aufruf der Adresse: <http://www.allgemeiner-datenschutz.de/analyze/index.htm>. Der Autor dieser Zeilen verbürgt sich übrigens dafür, dass dieser Test keinerlei Risiken oder Gefahren birgt. Lediglich ein bisschen Verwunderung könnte die Folge sein. Nach diesem Test könnte es nämlich sehr leicht passieren, dass Sie sich plötzlich intensiv für die Sicherheitseinstellungen Ihres Computers interessieren.

Jeder Benutzer zieht im Internet eine Spur von Daten hinter sich her, auf die kaum Einfluss zu nehmen ist. Beim Abrufen von Web-Seiten werden Ihre Daten auf Web-Servern gespeichert. Diese Daten können nicht nur für statistische Zwecke genutzt werden, es lässt sich mittels dieser Daten auch konkret zurückverfolgen, wer Sie sind. Damit ist nicht nur Ihr Alias-Name bei Ihrem Netzanbieter gemeint, sondern konkret Ihre Postanschrift, Ihr echter Name und Ihre Surf-Gewohnheiten.¹

Ein kleines Beispiel soll den Praxisbezug zur Schulbibliothek verdeutlichen: Ein Schüler benutzte in der Schulbibliothek ein Arbeitsgerät, auf dem ein E-Mail-Konto der Schulbibliothek eingerichtet war. Da er gerade keinen Unterricht besuchte, ging er ans Werk und verschickte E-Mails und SMS an unterschiedlichste Adressaten. Nachdem er seinen alltäglichen Kommunikationsverpflichtungen nachgekommen war, stellte sich in Anbetracht noch nicht gänzlich erschöpfter zeitlicher Ressourcen seine Kreativität und Experimen-

tierfreudigkeit ein. So unterrichtete besagter junger Mann ein durchaus bekanntes Medienunternehmen in allen Details davon, dass sich in allernächster Zukunft eine Katastrophe unermesslichen Ausmaßes an einem öffentlichen Ort ereignen werde ...

Es dauerte, wie sich vermuten lässt, nicht allzu lange, bis die Exekutive diesem Hinweis nachging und in späterer Folge auch dem Hinweisgeber auf die Spur kam. Der Rechner, von dem aus die Nachricht abgeschickt worden war, konnte jedenfalls einwandfrei identifiziert werden.

Besagter Fall – der sich tatsächlich so zutrug – hat in medienpädagogischer Hinsicht jedenfalls zu einer neuen Einschätzung geführt. Ebenfalls mit unliebsamen Folgen müssen Computerbenutzer rechnen, die allzu arglos auf dem Datenhighway unterwegs sind. Das Ausspionieren von Informationen auf Computern, Angriffe auf Hardware oder Software richtet sich nicht mehr ausschließlich auf kommerzielle Unternehmen, sondern macht auch vor den Systemen von Privatleuten oder Bildungseinrichtungen nicht Halt.

Datensicherheit und Datenschutz sind somit auch für Computer-Arbeitsplätze in Schulbibliotheken unerlässlich.

Sicherheitskonzept für die Schulbibliothek

An den Schulen gibt es in aller Regel ein Informatik-Kustodiat oder einen Informatik-Beauftragten, der ein Sicherheitskonzept für das EDV-Netzwerk der Schule entwickelt hat. Die Computer-Arbeitsplätze in der Schulbibliothek sollten in das Konzept eingebunden sein, Schulbibliothekar und Informatiker dann dieses Konzept gemeinsam besprechen. Das erspart einerseits unnötigen Ärger, andererseits aber auch kostbare Arbeitszeit. Vor allem aber gewährleistet ein gutes Sicherheitskonzept die Funktionalität und damit die Verfügbarkeit von Computern.

Die Bedrohungen und Gefahren sind vielfältig. Laut einer aktuellen Studie dauert es kaum mehr als 10 Minuten, bis ein ungeschützter PC im Internet durch Viren oder Trojaner befallen wird. Hat sich ein solcher Schädling erst einmal ins Netzwerk eingeschlichen, so verbreitet er sich rasch von einem Gerät zum nächsten. Daneben sind es auch immer wieder die Computerbenutzer selbst, die durch die Installation von Programmen oder durch originelles Ausprobieren

dessen, was sie zu Hause lieber nicht tun würden, Computersysteme ins Wanken bringen.

Soll man deswegen womöglich auf Computerarbeitsplätze in der Schulbibliothek verzichten? – Keineswegs. Die Kombination von Printmedien und digitaler Infrastruktur ermöglicht in der multimedialen Schulbibliothek einen modernen, auf Einbindung vielfältiger Medien gründenden Unterricht, der in seiner Attraktivität von den Schülern überaus geschätzt wird.

Was tun, sprach Zeus

Im Folgenden finden Sie daher eine Checkliste mit Tipps zur Datensicherheit, wie Computer in Ihrer Schulbibliothek abgesichert sein sollten:

Provider im Bildungsbereich haben normalerweise eine Firewall installiert, die den Aufruf von Webseiten mit gefährlichem Inhalt blockt. Zusätzlich empfiehlt sich auch an der Schule die Einrichtung einer Firewall, um Ihren Rechner vor unbefugten Zugriffen von außen zu schützen. Der Vorteil einer schuleigenen Firewall-Lösung besteht darin, dass sie individuelle Sicherheitseinstellungen ermöglicht, die im Normalfall weitaus restriktiver sind als die von Providern. Installieren Sie unbedingt einen Virenschoner, um Ihre PCs vor Computerviren zu schützen. Vergessen Sie nicht auf regelmäßige Updates für Ihren Virenschoner, was in aller Regel automatisiert erfolgen kann. Installieren Sie zusätzlich einen Trojanerschutz.

Überprüfen Sie die Sicherheitseinstellungen des Browsers (z.B. Internet Explorer, Opera etc). Regelmäßig sollten die neuesten Updates und Patches für Ihren Browser von der Webseite des Herstellers besorgt und installiert werden. Diese schließen oftmals bekannt gewordene Sicherheitslücken in der Browsersoftware.

Deaktivieren Sie Ihre Netzwerkfreigaben oder vergeben Sie auf jeden Fall Passwörter für die freigegebenen Ressourcen. Auf diese Ressourcen kann ansonsten mitunter auch von außen zugegriffen werden.

Sichern Sie Ihre sensiblen Daten – z.B. die Datenbank der Schulbibliothek – regelmäßig auch auf einem externen Datenträger ab (CD-ROM oder Zip-Disk). Wer absolut sicher gehen möchte, bewahrt ein aktuelles Backup auf einem externen Datenträger im Schulsafe oder außerhalb des Schulgebäudes auf.

Achten Sie auf sichere Passwörter. Ihr Lieblingsautor sollte dabei nicht als Passwort herhalten. Am besten eignet sich eine zufällige Reihenfolge aus Buchstaben, Zahlen und Sonderzeichen von wenigstens acht Stellen. Die Schwierigkeit besteht oft darin, dass man für verschiedenste Anmeldungen im Internet auch unterschiedliche Passwörter verwendet, deren Zuordnung einem dann mitunter

selbst Mühe bereitet. Dennoch sollten Passwörter niemals in eine Datei geschrieben werden, die auf dem Computer gespeichert wird. Richten Sie keine E-Mail-Konten mit den Daten der Schulbibliothek ein. Ansonsten könnte auch mit der Absenderadresse Ihrer Schulbibliothek Unfug getrieben werden.

Wussten Sie übrigens, dass das Löschen von Dateien auf dem Computer – dasselbe gilt auch für den Speicherchip von digitalen Kameras – kein endgültiges Löschen bedeutet? Selbst wenn Sie den Papierkorb geleert haben, lassen sich die vermeintlich gelöschten Daten mit relativ geringem Aufwand wiederherstellen. Endgültig gelöscht sind Daten erst dann, wenn der Datenträger gänzlich neu formatiert oder ein spezielles Löschmodul verwendet wurde.

Tipp zum Abschluss

Die Schülerarbeitsgeräte in meiner Schulbibliothek sind mit der Software HDGUARD gesichert. Das bedeutet, dass beim Neustart eines Computers die Festplatten-Partition C:\ auf den ursprünglichen Zustand rückgesetzt wird und allfällige Änderungen verloren gehen. Auf einer Partition D:\ hingegen dürfen Daten von Benutzern abgespeichert werden. Mit wenigen Mausklicks und mittels Passwort gesichert kann ein Administrator den Schutz aufheben, um z.B. ein neues Programm auf der C:\-Partition zu installieren. Danach greift wieder die Schutzfunktion. Diese Anschaffung hat den Wartungsaufwand an den Schulrechnern signifikant verringert, in gleichem Maß aber die Funktionalität gesteigert und vor allem viel Zeit und Nerven gespart. Es geht an dieser Stelle nicht um die Bewerbung einer Software – vergleichbare Produkte und Angebote sollten in Computerfachgeschäften nachgefragt werden –, sondern lediglich um einen Erfahrungsbericht im Hinblick auf die Lösung von Problemen, die in einer Schulbibliothek allgegenwärtig sind. Mit Sicherheit.

Fußnote:

1) Vgl. online im Internet: URL: <http://www.allgemeiner-datenschutz.de/analyze/index.htm> (Stand Mai 2005)



► Empfohlene Adressen im Internet:

www.univie.ac.at/ZID/gratissoftware/

www.virenschutz.info, www.trojaner-info.de

► **Mag. Jürgen Rathmayr** arbeitet für den Bibliotheken-Service für Schulen bei Buch.Zeit Wels und ist Mitglied der AG multimediale Schulbibliothek.