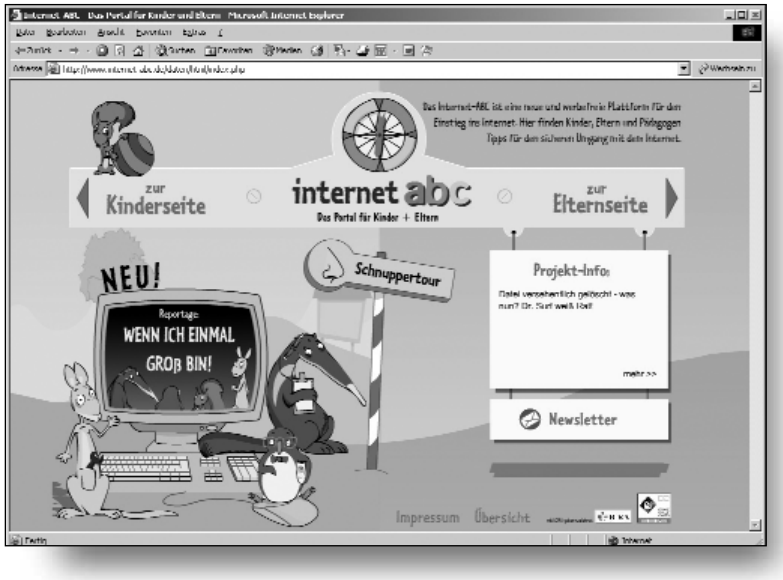
Gefahren aus dem Netz

Sicherheitsrisiken im Internet

Autorin: Gudrun Friedrich

„Die Schaffung eines ungehinderten Zugangs zum Internet durch Bibliotheken und Informationsdienste unterstützt Gemeinschaften und das Individuum beim Streben nach Freiheit, Wohlstand, Entwicklung."[1]

Immer mehr österreichische Bibliotheken bieten ihren KundInnen einen kostenlosen (oder kostengünstigen) Zugang zum Internet an und gewinnen so neue NutzerInnen-Gruppen. Neben ungeahnten Chancen für die Informationsgesellschaft bringt die Einführung des Internets allerdings auch neue Herausforderungen mit sich. „Viren, Würmer, Dialer" sind nur allzu bekannte Schlagworte zu den Schattenseiten des WWW. Kinder und Jugendliche sind durch ihre Unerfahrenheit besonderen Risiken ausgesetzt. Dieser Artikel will Ihnen ein Basiswissen über Gefahren aus dem Netz vermitteln und aufzeigen, wie Sie die Sicherheit in Ihrer Bibliothek erhöhen können. Die genannten Produkte und Links sind beispielhaft aufgeführt, es wird kein Anspruch auf Vollständigkeit erhoben.



▸ Viele Webseiten informieren über Sicherheitsmaßnahmen in Internet

Viren, Würmer & Co

Sie können sich **Viren** per E-Mail, Datenträger oder beim Surfen im Internet einfangen. Diese Schad-Programme infizieren andere Dateien, indem sie sich in ihnen einnisten. Viren können Dateien und Software löschen oder unbrauchbar machen. Ein Virenschutzprogramm ist daher unerlässlich – am besten eines, das sich regelmäßig automatisch auf den neuesten Stand der Virenabwehr bringt (s. „Technische Maßnahmen").

▸ **Links:**

http://www.computerviren-info.de
Was Sie über Computerviren wissen sollten
http://www.symantec.com/region/de/avcenter/
Antiviren-Forschungs-Zentrum mit aktuellen Warnungen und Regeln für sicheres Surfen

Ein **Wurm** ist ein bösartiger Virus. Er benötigt im Gegensatz zum Virus keinen Wirt. Er schleicht sich über den Anhang einer E-Mail oder über offene Ports[2] ins Computersystem ein. Unbemerkt verschickt er sich dann selbst per E-Mail weiter und kann ganze Rechnernetze lahm legen.

Bei **Hoaxes** (altengl. für Scherz) handelt es sich um eine gezielte Falschmeldung per E-Mail, die vor einem Virus oder Wurm warnt. Sie werden gebeten, diese Mail an FreundInnen und Bekannte weiterzuleiten, was zur Überlastung des Mailservers führen kann. Oder Sie werden aufgefordert, bestimmte Systemdateien zu löschen, und das kann Ihren Rechner lahm legen.

▸ **Links:**

http://www.hoax-info.de
Hoax-Info Service
http://www.tu-berlin.de/www/software/hoaxlist.shtml
Hier finden Sie Hoax-Listen

Trojaner (Trojanische Pferde) sind Programme, die unbefugten Personen Zugriff auf den eigenen Rechner ermöglichen. Eine Sonderform sind Werbe-Trojaner, so genannte Spyware, die man sich meist als Zugabe zu einer kostenlosen Software herunter lädt. Über Trojaner kann das Surfverhalten von InternetnutzerInnen ermittelt werden – bis hin zum Ausspähen von Passwörtern und Kreditkartennummern.

▸ **Links:**

http://www.trojanerinfo.de/

Information zu den neuesten Trojanern, Viren und Würmern

www.lavasoft.de

Download des kostenlosen Programmes „Ad-Aware"

http://download.freenet.de/archiv_s/spybot_search_und_destroy_4656.html: Download der Freeware „Spybot Search&Destroy"

Dialer – automatische Telefonwählprogramme – werden dazu missbraucht, Internetverbindungen auf Mehrwertnummern oder Auslandsrufnummern umzuleiten. Als „Flaterate"[3]-SurferIn (Chello, ADSL) können Sie sich hier weitgehend sicher fühlen.

▸ **Links:**

http://www.dialer-control.de

Kostenloses „Dialer-Control"-Programm

http://www.bsi.de/av/dialer.htm

Dialer-Info des Deutschen Bundesamts für Sicherheit in der Informationstechnik

Technische Maßnahmen

Sicherheit im Internet fängt bei Ihrem Browser an. Es bedarf nur weniger Einstellungen, um hier das Sicherheitsrisiko zu verringern. Die höchste Sicherheitsstufe wiederum kann bedeuten, dass viele Internetseiten nicht mehr funktionieren.

Einen Browser-Check für die gängigsten Browser finden Sie unter http://www.heise.de/ct/browsercheck. Sie werden Schritt für Schritt durch die wichtigsten Einstellungen geführt und auf Sicherheitslücken aufmerksam gemacht.

Da die Microsoft-Produkte am weitesten verbreitet sind, richten sich viele Attacken gegen sie. Laden Sie sich regelmäßig unter http://www.microsoft.com/downloads die kostenlosen Sicherheits-Updates („Patches"[4]) herunter. Oder wählen Sie direkt im Browser Internet Explorer im Menü „Extras" den Punkt „Windows Update" an.

▸ **Links:**

http://www.sicher-im-internet.at

Portal zur Erhöhung der IT-Sicherheit in Österreich; unterstützt u.a. vom BM für Bildung, Wissenschaft und Kultur

Zur Grundausstattung jedes Internet-Rechners gehören heute ein Virenschutzprogramm und eine Firewall. Die Antiviren-Software kontrolliert die per E-Mail oder über die Internetverbindung ein- und ausgehenden Daten. Die Firewall (dt. „Brandschutzmauer") verhindert, dass Hacker oder Cracker[5] auf Ihr System von außen zugreifen.

▸ **Links:**

http://www.kaspersky.com, http://www.mcafee.at, http://www.symantec.at

Links zu kommerziellen Virenschutzprogrammen

http://www.free-av.de

Kostenfreier Virenschutz „AntiVir" für PrivatanwenderInnen

http://www.zonelabs.com

Kostenlose Firewall für den privaten Gebrauch

Um öffentlich zugängliche Rechner sowohl vor Viren als auch vor Manipulationen auf BenutzerInnen-Seite (Löschen von Verzeichnissen, Herunterladen von Programmen aus dem Internet etc.) zu schützen, haben sich so genannte Protektorkarten als nützlich erwiesen. Diese „frieren" die Originalkonfiguration des Computers ein und stellen sie bei jedem Neustart wieder her.

▸ **Links:**

http://www.dr-kaiser.de, http://www.hdd-sheriff.de, http://www.daten-airbag.de

Kommerzielle Anbieter von Protektorkarten

Es gibt kein Patentrezept zum sicheren Umgang im Netz. Technisches Detailwissen ist erforderlich und die AnwenderInnen müssen sich auf dem Laufenden halten. Mit der Sensibilisierung für mögliche Gefahren ist schon einiges erreicht. Und es gibt weitere Risikobereiche im Internet …

Problematische Angebote

Vor allem im Hinblick auf Kinder und Jugendliche ist das Internet durch Websites von unseriösen Anbietern (Pornografie, Rechtsextremismus, Gewaltverherrlichung/Gewaltverharmlosung, „Tasteless Seiten" etc.) problematisch.

Als Lösungsansätze bieten sich hier an:

„Soziale Kontrolle", d.h. die Internet-PCs werden so aufgestellt, dass sie jederzeit von BibliotheksmitarbeiterInnen und von KundInnen eingesehen werden können.

Nutzungsvereinbarungen mit klaren Regeln für die Nutzung des Internets und Sanktionen (Computerverbot, Hausverbot) bei Missbrauch.

Filtersysteme: Das sind Computerprogramme, welche verhindern, dass bestimmte Internetinhalte aufgerufen oder angezeigt werden können. Im Browser Internet Explorer lässt sich ebenfalls über Extras > Internetoptionen > Inhalte > Inhaltsratgeber eine Filterfunktion aktivieren.

▸ **Links:**

http://www.icra.org/icraplus:
Kostenloser Filter von ICRA
http://www.symantec.com/region/de/product/nis/se_indexseite.html
Die Software „Norton Internet Security" bietet u.a. auch eine Filterfunktion.
http://www.fh-merseburg.de/~wwwbib/oebib/Filter.html
Wirkungsweise und Problematik von Filtersoftware
http://www.internet-abc.de/daten/html/Eltern/html/bibliothek/-bibliothek_medienkompetenz_index.php
Bei „Sicher im Netz" finden Sie Informationen über Filter.

Da technische Lösungen wie Filterprogramme oft nur begrenzten Schutz bieten, ist es unerlässlich, dass BibliothekarInnen Ihren NutzerInnen umfassende Medienkompetenz vermitteln. Die Vermittlung von Kenntnissen technischer Natur ist hierbei genau so wichtig wie die in der Bewertung von Inhalten und Informationen.

▸ **Links:**

www.saferinternet.at
Ziel der europäischen Kampagne „SaferInternet" ist die Förderung der Medienkompetenz.

Literatur:

Lindhorst, Arno: Das Einsteigerseminar Sicherheit im Internet / Arno Lindhorst. - Bonn : bhv, 2002.
C't : Magazin für Computertechnik. Hannover : Heise. - (Online unter http://www.heise.de).

Fußnoten:

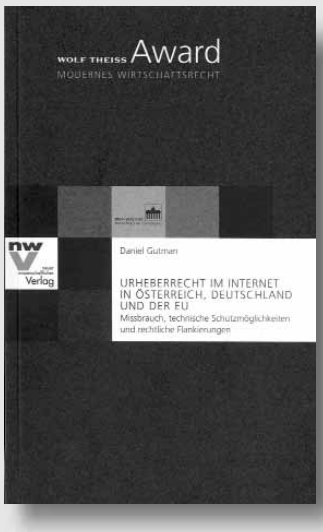
1) www.ifla.org/III/misc/im-g.htm (23.4.2005)
2) TCP/IP-Schnittstelle zum Internet
3) Internetzugang zu einem Pauschalpreis
4) Engl. flicken
5) Cracker sind „böse" Hacker, die Sicherheitslücken im Internet nicht nur aufzeigen, sondern diese für ihre Zwecke missbrauchen.

▸ **Weitere Informationen:**
Gudrun Friedrich
Büchereiverband Österreichs, Tel.: 01/406 97 22-23
E-Mail: friedrich@bvoe.at

Urheberrecht im Internet in Österreich, Deutschland und der EU

Autorin: Anita Eichinger

Urheberrecht im Internet ist eine komplizierte Materie und so ist die Literatur zu diesem Thema umfangreich und in vielen Fällen – zumindest für Laien – oft ebenso kompliziert. Eine wunderbare Ausnahme bildet das vorliegende Buch von Daniel Gutman.



Einleitend gibt der Autor einen Überblick über die technische Seite des Internets, um anschließend auf die historische Entwicklung des Urheberrechts einzugehen.
Ausgehend von der EU-Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts aus dem Jahr 2001 stellt Gutman sodann die Probleme des Urheberrechts im Internet dar, und zwar sowohl für Österreich als auch für Deutschland. Dem Bereich der Urheberrechtsverletzungen (Raubkopien!) ist dabei ebenso Raum gewidmet wie den Schutzmöglichkeiten.
Am Ende des Buches weiß jede/r Leser/in, was nun eigentlich im Internet erlaubt ist und was nicht. Welche Konsequenzen daraus zu ziehen sind, muss jede/r Leser/in natürlich für sich selbst entscheiden!

Gutman, Daniel: Urheberrecht im Internet in Österreich, Deutschland und der EU : Missbrauch, technische Schutzmöglichkeiten und rechtliche Flankierungen / Daniel Gutman. - Wien [u.a.] : nwv, 2003. - 207 S. - (Wolf Theiss Award ; 3)