Computer- und Internetsicherheit

Schätzungen prominenter Suchmaschinen zufolge gibt es weltweit über eine Billion Webseiten und es wird vermutet, dass diese Zahl täglich um mehrere Hundertausend anwächst. Man geht davon aus, dass etwa 1,5 Milliarden Menschen das Internet benutzen. Somit zählt das Internet zu den größten Erfolgsgeschichten der Menschheit. Es dient uns als Anlaufpunkt für Informationen und Unterhaltung und wir können es als unser Sprachrohr und Werkzeug zur Selbstpräsentation nutzen.

In den letzten Jahren hat sich ein tiefgreifender Paradigmenwechsel im WorldWideWeb vollzogen. Während früher die Grenze zwischen Produzent und Konsument klar erkennbar war, wurde diese durch die Revolution des Web 2.0 immer weiter aufgelöst. Auch ohne tiefgreifende technische Kenntnisse ist es sehr leicht, eigene Inhalte im Netz zu veröffentlichen. Egal ob es um Text (Twitter, Blogs, Facebook und Co.), Fotos (Picasa, Flickr) oder Videos (Youtube, MyVideo) geht – jeder kann und soll mitmachen.

Problematik

All diese Entwicklungen haben allerdings auch dazu geführt, dass das Internet ein Sammelbecken für eher zweifelhafte Inhalte wurde. Man findet Homepages mit pornografischem Inhalt, offener Gewaltdarstellung, nationalsozialistischem Inhalt, Beleidigungen und Diffamierungen wie Sand am Meer.

Problematisch wird diese Situation vor allem dann, wenn man Kindern und Jugendlichen die Möglichkeit bieten will, das Internet zu erkunden. Einerseits sollte man Ihnen den Zugang zum Medium Internet keinesfalls verwehren – andererseits will man allerdings auch nicht, dass sie mit unangemessenen Inhalten konfrontiert werden. Schon früh wurde deshalb der Ruf nach Filtermöglichkeiten für das Internet laut. So gibt es mittlerweile eine große Anzahl an freier und kostenpflichtiger Filtersoftware. Dabei gibt es sowohl Spezialsoftware (WinTimer[1], Net Nanny[2], Safe Eyes[3], CYBERsitter[4]), als auch Zusatzmodule von gängigen Anbietern von Virensoftware (Avira[5], McAffee[6], Kaspersky[7]).

1 http://www.wintimer-kindersicherung.de/
2 http://www.netnanny.com/
3 http://www.internetsafety.com/safe-eyes-parental-control-software.php
4 http://www.cybersitter.com/
5 http://www.avira.com/de/pages/index.php
6 http://home.mcafee.com/
7 http://www.kaspersky.com/de/

Filtersoftware

Von der Funktionsweise her arbeiten solche Filter nach sehr ähnlichen Prinzipien – einer redaktionellen Klassifizierung, einer automatischen Klassifizierung oder durch eine Selbstklassifizierung durch den Anbieter.

Bei der redaktionellen Klassifizierung gibt es sogenannte „Blacklists“ und „Whitelists“. Als Blacklist versteht man eine Liste von Internetseiten, die gesperrt sind. Sobald also der Benutzer eine dieser Seiten ansteuert, schaltet sich der Filter ein. Das Gegenstück dazu sind die Whitelists. In diesen Listen sind Seiten angeführt, die angezeigt werden dürfen. Diese Vorgehensweise wird oft noch mit einer automatischen Klassifizierung gekoppelt. Dabei wird eine Seite nach Schlüsselwörtern durchsucht. Wird ein solches Schlüsselwort gefunden und die Seite steht nicht auf der Whitelist, dann wird die Seite auch nicht angezeigt. Die dritte Möglichkeit besteht in der Klassifizierung durch den Anbieter der Homepage. Dieser versieht seine Homepage mit einer virtuellen Kennzeichnung, die von der Filtersoftware erkannt wird. Bei der Verwendung von Filtersoftware entscheidet man also, welche Seiten-Klassen geblockt bzw. erlaubt sind. Solche Klassen können zum Beispiel sein: Gewalt, Waffen, Hass, Sex, Beschimpfungen, ...

Diese Vorgehensweisen bringen allerdings so manche Probleme mit sich. Zum einen ist es durch die Dynamik des Mediums Internet zwingend notwendig, dass die Listen ständig gepflegt und erweitert werden. Wenn täglich tausende neue Seiten mit problematischem Inhalt online gehen, dann müssen diese Seiten natürlich auch in die Blacklists eingetragen werden. Die Aktualisierungen dieser Listen lassen sich die Hersteller der Filtersoftware allerdings gut bezahlen. Ähnlich einem Abo kann man für unterschiedliche Zeiträume das Recht auf Bezug der neuen Listen kaufen.
Ein zusätzliches Problem tritt dadurch auf, dass viele dieser Filter von Firmen aus den USA produziert werden. Diese sind oft sehr restriktiv, wenn es um die Filterung von sexuellem Inhalt geht, was wiederum dazu führt, dass auch Aufklärungsseiten blockiert werden. Andererseits sind die amerikanischen Filter sehr tolerant gegenüber Seiten mit nationalsozialistischem Inhalt.

Monitoring-Software

Sehr interessant ist in diesem Bereich noch ein anderer Ansatz. Es ist dies die Monitoring-Software. Dabei handelt es sich um Programme, die sämtliche Aktivitäten auf einem PC verfolgen und protokollieren. Verbreitete Anbieter sind hier beispielsweise „Orvell Monitoring 2010[8]“, „Spector Pro[9]“ oder „Winston Monitoring[10]“. Je nach Funktionsumfang der Software werden hier verschiedenste Aktivitäten aufgezeichnet: Besuchte Webseiten, gestartete Anwendungen, Tastenanschläge, Anschluss von USB-Geräten, geschriebene Emails, Messenger-Chats (ICQ, Skype, ...). Diese Überwachung geht teilweise sogar soweit, dass bei verdächtigen Aktivitäten mit einer Webcam ein Foto des Benutzers gemacht wird.

8 http://www.protectcom.de/orvell/de/
9 http://www.spectorsoft.com/products/SpectorPro_Windows/entry.asp
10 http://www.protectcom.de/winston/de/

Diese Vorgehensweise hat sowohl Vorteile als auch Nachteile. Der Nachteil ist mit Sicherheit, dass ich den Besuch von problematischen Seiten nicht verhindern kann, da ich die Information darüber erst im Nachhinein erhalte. Zusätzlich ist die Auswertung der Informationen mit einem gewissen Aufwand verbunden. Auch ist es unbedingt notwendig, die Jugendlichen oder Schüler darüber zu informieren, dass sämtliche Aktivitäten aufgezeichnet werden. Vor allem auch deshalb, weil durch die Aufzeichnung der Tastenschläge theoretisch auch Benutzernamen und Passwörter eruiert werden können. Erfahrungsgemäß vermindert die Information, dass die PC-Aktivitäten protokolliert werden die ungewollte Nutzung auch nur dann, wenn man Verstöße dagegen auch wirklich ahndet. Dafür erhält man aber auch einen detaillierten Überblick, mit welchen Inhalten sich Jugendliche beschäftigen. Mit diesem Wissen wiederum kann ich ganz gezielt das Gespräch suchen und herausfinden, was den Jugendlichen veranlasst, problematische Inhalte zu konsumieren.

Umsetzung in der Schule

Sollten Sie in Ihrer Schule Probleme damit haben, dass Ihre Schüler auf unerwünschten Seiten unterwegs sind, können Sie als ersten Schritt Demo-Versionen von geeigneter Software installieren. Dadurch erhalten Sie die Möglichkeit, die unterschiedlichen Funktionsweisen kennenzulernen und müssen nicht die Katze im Sack kaufen. Im Idealfall wählen Sie ein Produkt, welches sowohl Filterfunktionen als auch das Monitoring beherrscht.

Nachdem Sie sich für ein Produkt entschieden haben, muss unbedingt geklärt werden, wie sich die Software auf den Schulrechnern installieren lässt. Es gibt Programme, die auf jedem Rechner einzeln verwaltet werden müssen und solche, die über ein Netzwerk zentral administriert werden können. Ein netzwerkfähiges, vom Funktionsumfang her sehr mächtiges Programm ist beispielsweise „IMLOCK Enterprise“ der Firma Comvigo[11]. Bei diesem Programm hat man sehr viele Möglichkeiten, Programme, Internetseiten oder Windows-Funktionen zu blockieren und erhält gleichzeitig Reports per Email oder über das Programm-Interface. Verwaltet kann alles zentral von einem Computer aus werden. Eine Testversion der Software erhalten Sie beispielsweise direkt auf der Homepage des Herstellers.

Wichtig ist hier natürlich, dass Sie nicht von Anfang an eine perfekte Software erwarten dürfen. Je größer der Funktionsumfang ist, desto mehr Einstellungsmöglichkeiten gibt es. Es muss einfach laufend festgelegt werden, welche Programme geblockt werden, die Blacklists und Whithelists gehören erweitert um die Seiten, die nicht vom Hersteller eingetragen sind und man muss natürlich festlegen, wie bzw. wie oft die Auswertungen bereitgestellt werden. Nicht unerwähnt soll bleiben, dass Schüler oft eine gewisse Herausforderung darin sehen, Filtersoftware zu umgehen oder zu deaktivieren. Bei moderner Software ist das zwar sehr schwierig – findet der Schüler allerdings das verwendete Passwort heraus, kann er sich wieder frei bewegen. Hier ist es also auch wichtig, sichere Passwörter zu verwenden (Buchstaben, Zahlen, Sonderzeichen) und das Passwort auch regelmäßig zu wechseln.

11 http://www.comvigo.com/

Fazit

Es lässt sich durch den Einsatz solcher Programme nie eine hundertprozentige Absicherung erreichen. Man darf sich nicht dazu verleiten lassen, diese Programme als digitalen Babysitter anzusehen. Viel wichtiger ist es, im Rahmen einer gezielten Medienerziehung dafür zu sorgen, dass Kinder und Jugendliche für die Gefahren des Internets sensibilisiert werden.
Zusammenfassend kann man also sagen, dass es den perfekten Schutz im Internet nicht gibt und wohl auch nie geben wird. Die verwendeten Technologien im WorldWideWeb wurden ganz bewusst so gewählt, dass sie sich nur sehr schwer kontrollieren und zensurieren lassen. Will man dieser Freiheit also im Namen des Jugendschutzes einen Riegel vorschieben, muss man leider hinnehmen, dass Schutzmechanismen immer Löcher aufweisen und man auch zukünftig nicht die Möglichkeit bekommen wird, die Erziehung unserer Kinder und Jugendlichen dem Internet zu überlassen. Der moralische und ethische Grundstock muss nach wie vor durch Institutionen wie Schule und vor allem Familie gelegt werden.

DI(FH) Bernhard Füchsl