Computer-Sicherheit und Internet

Das Thema Sicherheit ist mittlerweile schon fast jedem Internetbenutzer begegnet. Äußerst unterschiedlich sind allerdings die Schlussfolgerungen, die der einzelne für sein Verhalten daraus ableitet. Als Anregung, sich aktuell damit auseinander zu setzen möge der folgende Überblick dienen.

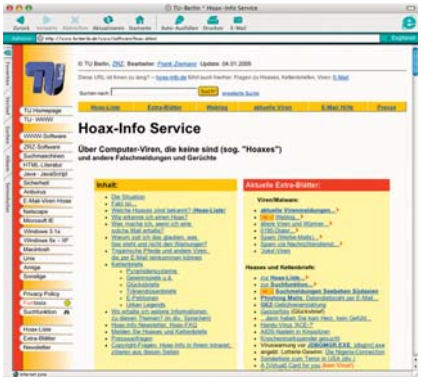
Folgende (tatsächliche) Begebenheit kann zur Verdeutlichung der derzeitigen Situation dienen. Mit einem soeben erworbenen Laptop kommt Kollege X nach Hause. Er freut sich schon, dort seinen kürzlich eingerichteten DSL-Anschluss nutzen zu können. Schnell ist die Konfiguration eingegeben und der Laptop am Netz. Die ersten Webseiten erscheinen tatsächlich sehr schnell am Bildschirm. Nun will er noch die nötigen Service Packs und Updates laden. Dabei bleibt der Rechner hängen – nichts geht mehr. Auch ein Neustart gelingt nicht. Im folgenden Wiederherstellungsversuch, der die Unterstützung des Händlers nötig macht, stellt sich heraus, dass der Rechner in der kurzen Onlinezeit bereits mit mehreren Viren verseucht wurde, die eine Wiederherstellung wesentlich erschwerten.

Das ist nur ein Beispiel für die derzeitige Situation. Andere Risiken bergen beispielsweise E-Mails, die Webadressen enthalten und beim Anklicken nur scheinbar eine vertraute Seite auf den Bildschirm holen. Eingaben auf dieser Seite landen dann oft in unseriösen Händen.

Wesentlich harmloser sind da schon Hoaxes (vom englischen Scherz, Schwindel), das sind E-Mails, deren Inhalt einen zur Weiterleitung motivieren soll. So entsteht dann eine Lawine von Millionen E-Mails, die in der Summe Teile des Internets schwer beeinträchtigen können. Von Hilferufen bis zu kostenlosen Handys reicht das Spektrum der Inhalte dieser manchmal sehr plausiblen Schein-Nachrichten. Oft sehen diese Nachrichten sogar authentisch aus. Allerdings ist zu bedenken, dass weder Antivirensoftwarehersteller noch Regierungsbehörden oder Hilfsorganisationen unangeforderte Massenaussendungen erstellen und um deren Weiterleitung bitten, allein schon deshalb, weil deren Aktualität dann nicht mehr garantiert werden kann und zudem der Ruf der jeweiligen Organisation Schaden nimmt.

Erste Anlaufstelle bei Unsicherheiten ist da ein aktuelles Verzeichnis der bekannten Störnachrichten und gängiger Strömungen wie es die TU Berlin anbietet. www.tu-berlin.de/www/software/hoax.shtml

Umfangreiche Detailinformationen zu aktuellen Sicherheitsproblemen werden hier gesammelt und kommentiert. www.securityfocus.com/



Ein Verzeichnis aller aktuellen Störnachrichten, Erklärungen und aktueller Tendenzen findet man bei der TU-Berlin unter: www.tu-berlin.de/www/software/hoax.shtml

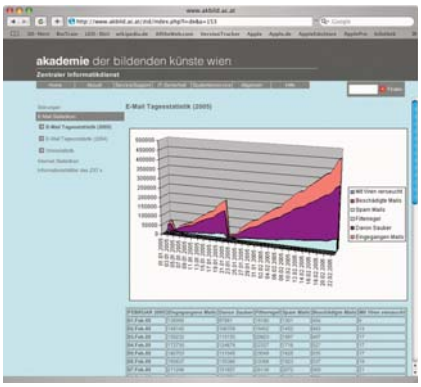
Eine sehr gute Einstiegsseite bietet das Bundesamt für Sicherheit in der Informationstechnik. Dort werden alle relevanten Themen verständlich erläutert und auch Maßnahmen und Sicherheitswerkzeuge angeboten.
www.bsi-fuer-buerger.de/internet/index.htm

Anti-Virensoftwarehersteller bieten Informationen über aktuelle Viren und eine Einschätzung des Gefahrenpotenzials auf ihren Webseiten. Hier finden sich auch Updates für die jeweilige Software, die nötig sind, um auch aktuelle Viren auf dem Rechner finden und ausschalten zu können.

http://de.mcafee.com/virusInfo/default.asp
http://securityresponse.symantec.com/
http://secunia.com/
www.sophos.de/
http://ca.com/de/

Eine gute Übersicht zu Viren, Software für Windows, Mac OS und Linux sowie Gegenmaßnahmen findet sich unter: www.tu-berlin.de/www/software/antivirus.shtml#univ.

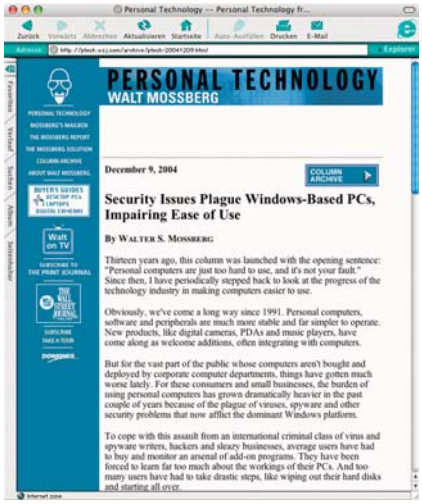
Ob und wie gefährdet der eigene Web-Browser ist, hängt von den jeweiligen Einstellungen ab. Der Heise Verlag bietet Tipps zur sicheren Konfiguration sowie Hinweise und Berichte zu Sicherheitsthemen. www.heise.de/security/dienste/browsercheck/



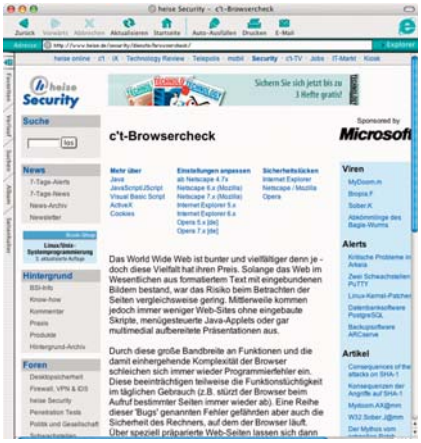
Um sich einen Eindruck zu verschaffen, was täglich mit Mail transportiert wird kann man einen Blick auf die Statistiken der Akademie der Bildenden Künste werfen.
www.akbild.ac.at/zid/index.php?l=de&a=153.

Lohnend ist auch der Blick in andere Computerzeitschriften, die gelegentlich Schwerpunktberichte zu Sicherheitsthemen bringen. Wer sich von den zahlreichen Sicherheitsfragen überwältigt fühlt für den bietet diese Kolumne des Wall Street Journal den Trost, dass es vielen so geht und es auch Auswege gibt.
http://ptech.wsj.com/archive/ptech-20041209.html

Auch Microsoft warnt vor aktuellen Gefahren und Sicherheitslücken. Windows-Nutzer sollten sich dort regelmäßig auch über notwendige Patches, also Softwareaktualisierun-

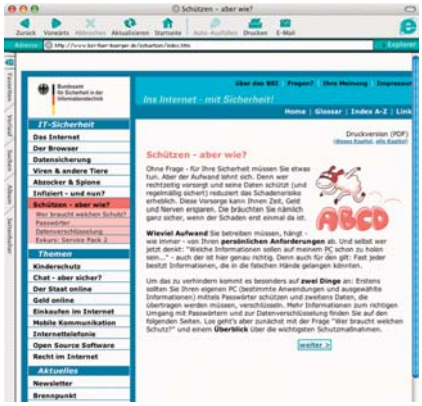


Auch das Wall Street Journal beschäftigt sich mit Computern und hat dafür eine eigene Kolumne eingerichtet. http://ptech.wsj.com/archive/ptech-20041209.html



Vorbeugen hilft. Jedenfalls ist man mit den korrekten Einstellungen für den jeweiligen Browser vor manchen Gefahren geschützt. Wie es geht wird beim Heise Verlag genau erläutert. www.heise.de/security/dienste/browsercheck/

Von Unsinn und E-Mail-Scherzen bis zu ernsten Themen finden sich Erläuterungen und geschichtliche Hintergründe hier gesammelt. Ziel ist die Vorbeugung der Massenhysterie, die auch im Internet zum Sicherheitsrisiko wird. www.vmyths.com/



Auch in Deutschland wurde eine IT-Sicherheitsbehörde eingerichtet, die eine Informationssammlung betreibt und Hilfestellung für alle Bürger gibt. www.bsi-fuer-buerger.de/internet/index.htm

Auch in den USA befasst sich eine Behörde mit diversen Sicherheitsthemen und dokumentiert alle bekannten Sicherheitslücken. http://ciac.llnl.gov/ciac/CIACHome.html

gen, oder notwendige Einstellungen informieren. www.microsoft.com/germany/ms/security/default.mspx

Beispielhaft für Gruppen und Privatpersonen, die zum Teil sehr explorativ und technisch Sicherheitsthemen bearbeiten seien folgende genannt. www.guninski.com/ www.shmoo.com/

Als Vorsichtsmaßnahmen haben sich folgende Grundregeln zur Computersicherheit bewährt:

1. **Aktualisieren** Sie Ihr Betriebssystem und natürlich besonders Ihren Virenscanner regelmäßig.
2. Öffnen Sie möglichst keine E-Mail oder Attachments, die Sie nicht angefordert haben und die von seltsamen Adressaten stammen. Stellen Sie Ihr Mailprogramm so ein, dass die angehängte Datei nicht automatisch geöffnet wird.
3. Laden Sie möglichst keine Daten von unbekannten oder zweifelhaften Internetseiten (zum Beispiel kostenloser Screensaver usw.). Notfalls überprüfen Sie diese mit dem Virenscanner sofort.
4. Versenden Sie **Dokumente möglichst im RTF-Format** (nicht DOC) und bitten Sie andere auch darum. So können keine Office-Makroviren verbreitet werden.
5. **Löschen** Sie unsinnige Mails und Kettenbriefe (nicht weiterleiten).
6. Öffnen Sie grundsätzlich keine Dateien, die mehr als eine Erweiterung haben, zum Beispiel Angebot.txt.exe.
7. Erstellen Sie regelmäßig **Sicherheitskopien** Ihrer wichtigen Daten.

Eine persönliche Sicherheitsstrategie ist heute unumgänglich, wenn man einen oder mehrere Rechner am Internet betreibt. Regelmäßige Sicherungen aller wichtigen Daten, die auch mit wenig Aufwand wiederhergestellt werden können sollten selbstverständlich sein. Der Zeitaufwand dafür lohnt sich zur Vorbeugung vor Datenverlust allemal. Erwähnung verdient hier der Einsatz alternativer Betriebssysteme, also Mac OS X von Apple und die verschiedenen Linux-Varianten (zum Beispiel Suse, RedHat, Debian und andere) die von ihrer gesamten Struktur wesentlich sicherer vor Angriffen aus dem Internet sind.

Anschrift des Verfassers:
Dr. Marc M. Batschkus, Multimedia-Lerncenter-Medizin, IBE-Klinikum Großhadern der Universität München,
E-Mail: bat@ibe.med.uni-muenchen.de
Internet: http://mmlc.web.med.uni-muenchen.de/mmlc.html