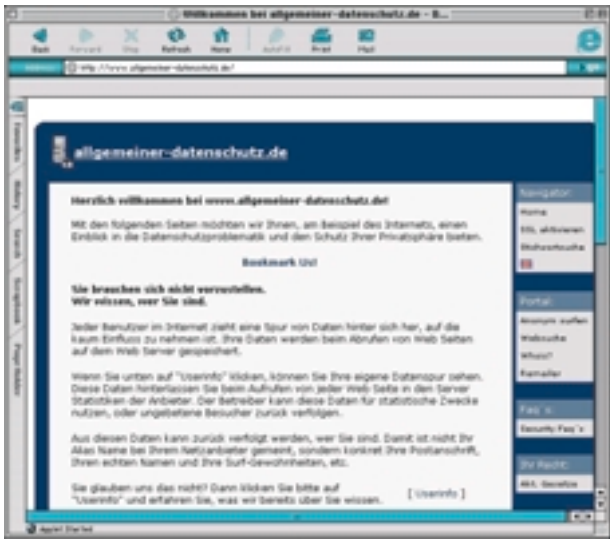
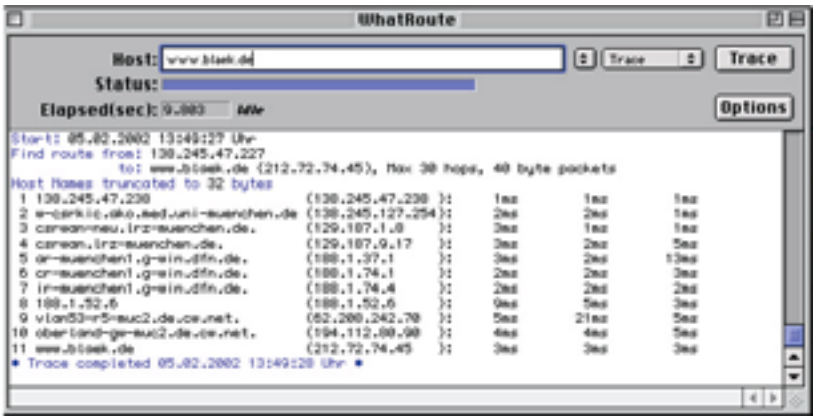
Sicherheit im Netz – nur Vorbeugen hilft

Der Web-Führerschein bietet Einstiegshilfe in Benutzung und Begriffe, die für Verständnis und sichere Nutzung unentbehrlich sind: http://web-fuehrerschein.web.de/



Jeder Internetnutzer erzeugt eine Datenspur. Was alles über Sie als Nutzer zu erfahren ist, können Sie hier selbst sehen: http://www.allgemeiner-datenschutz.de/



Jede Anfrage oder E-Mail durchläuft mehrere Rechner, sogar innerhalb einer Stadt. TraceRoute-Programme finden Sie unter: http://www.nettoolbox.com/, http://www.cyberkit.net/

Sicherheit im Internet wird immer mehr zum wichtigen Thema. Verschiedene Aspekte spielen dabei eine Rolle. Zum einen ist es die generelle „Abhörbarkeit" von E-Mails, da diese auf dem Weg zum Empfänger zahlreiche Rechner durchlaufen, die quasi als Umschaltstation dienen. Nur verschlüsselte Nachrichten sind hier sicher, sofern man nicht überhaupt in einem geschützten Netz arbeitet, wie zum Beispiel im Intranet des Deutschen Gesundheitsnetzes oder mit einem gesicherten Server verbunden ist (Adressen, die mit „https://..." beginnen).

Zum anderen geht es um den Schutz Ihres Rechners, der einerseits Angriffen aus dem Internet ausgesetzt ist, durch heruntergeladene Dateien, Mails etc. mit Viren und ähnlichem verseucht werden kann und zudem immer auch konventionellen Gefährdungen (Diebstahl, Wasser-, Stromschaden etc.) unterliegt. Richtige Einstellungen des Internet-Browsers und bedachtes Verhalten verringern dabei das Risiko erheblich.

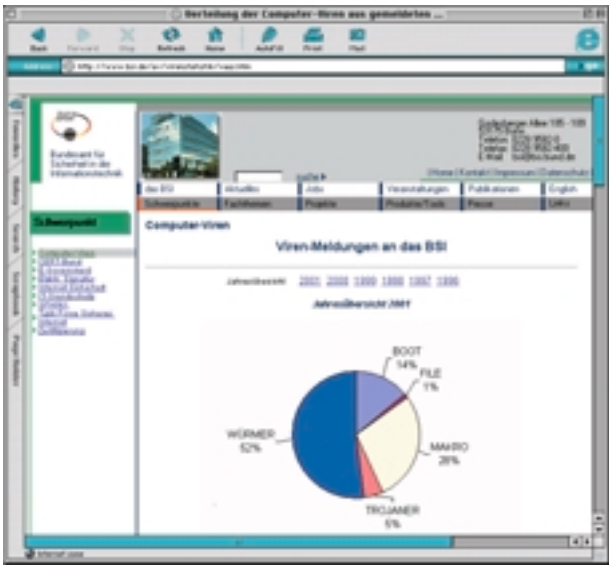
Ein guter Startpunkt für konkrete Informationen und Maßnahmen ist die Seite http://www.sicherheit-im-internet.de/ des Bundesministeriums für Wirtschaft und Technologie.

Offizielle Informationen, Richtlinien und Hilfestellungen sind beim Bundesamt für Sicherheit in der Informationstechnik erhältlich: http://www.bsi.de/.
Das Virtual Privacy Office sammelt relevante Informationen aus verschiedenen Ländern unter http://www.datenschutz.de/.

Zur Orientierung hier einige Grundregeln

Laden Sie möglichst keine E-Mail-Anhänge (Attachments) von Ihnen unbekannten Absendern. Löschen Sie am besten alle erkennbaren Werbemails ungeöffnet. Die Dateiart kann nicht sicher über das Bildsymbol erkannt werden, da dieses besonders bei Viren oder Ähnlichem getarnt wird. Alle ausführbaren Dateien (*.COM, *.EXE, *.VBS, *.BAT), Office-Dateien (*.DOC, *.XLS, *.PPT) und Bildschirmschoner (*.SCR) bergen Gefahrenpotential. Am sichersten sind Sie vor allen Gefahren, wenn Sie von den wichtigen Dokumenten auf Ihrem Rechner regelmäßig ein Backup (auf CD-R, ZIP, DAT, DVD-R oder Ähnlichem) erstellen und dieses räumlich auslagern.

Mit einigen Tests können Sie herausfinden, ob sie über das www angreifbar sind und wie Sie sich schützen können: http://www.heise.de/ct/browsercheck/



Elektronische Parasiten bestehen aus verschiedenen Gattungen und Gefahrenklassen vom harmlosen Scherz bis zur totalen Datenzerstörung: http://www.bsi.de/av/virenstatistik/vaus.htm

Effektiver Virenschutz ist nur zu gewährleisten, wenn neben dem Virenschutzprogramm auch die monatlichen Updates bzw. Virendefinitionsdateien installiert werden. Da viele Viren auf Microsoft Outlook aufbauen, kann durch Einsatz eines anderen Mail-Programmes die Anfälligkeit reduziert werden.

Aktuelle Virenwarnungen und Anti-Viren-Software finden Sie unter:
http://www.drsolomon.com/
http://www3.ca.com/virus/
http://securityresponse.symantec.com/avcenter/vinfodb.html/
http://www.sophos.com/

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