ecmc

Sicherer Surfen

1. Woran Sie beim Surfen immer denken sollten!

Generell gilt: Blindes Vertrauen im Internet ist fehl am Platz. Gehen Sie vorsichtig mit Ihren persönlichen Daten um und erneuern Sie Ihre Passwörter in regelmäßigen Abständen. Beachten Sie dabei, dass z.B. Ihr Vorname oder der Name eines Familienangehörigen kein wirklich sicheres Passwort ist.

Falls Sie sich nicht immer alle Zugangsdaten merken können oder wollen, benutzen Sie Passwort-Tresore. Sie können Ihnen bei der sicheren Verwaltung und auch beim Erstellen neuer Passwörter helfen. Die hier aufgeführten Produkte sind Freeware, in ihrer Benutzung also kostenlos.

- Password Gorilla http://www.fpx.de/fp/Software/Gorilla
- Passwort.Tresor http://www.passworttresor.de/download.php3
- Passwort Generator http://www.atory.com/Password_Generator/

Sie müssen kein Computerfreak sein, um sich ein wenig mit der Sicherheit Ihres Rechners zu befassen. Bedenken Sie, dass die rapide Verbreitung von Viren vorwiegend dadurch zustande kommt, dass sorglose Computernutzer ihre Systeme nicht genügend absichern. Vertrauen Sie außerdem nicht darauf, dass Ihr System vollkommen sicher ist, nur weil Sie ein Anti-Virenprogramm und eine Firewall installiert haben. Denn eine hundertprozentige Sicherheit ist nicht erreichbar. Es wird immer eine noch nicht erkannte Lücke oder einen neuen Virus geben, der Ihr System befallen kann.

Ein großer Vorteil der regelmäßigen Pflege Ihres Betriebssystems liegt darin, dass Sie sicherer und kompetenter im Umgang mit Computer werden, Software und Internet immer sicherer einschätzen können. Damit wird ein ausgewogener Umgang mit dem Medium möglich – weder gefährliche Unbedarftheit noch übersteigerte Panik.

2. Hat Ihre Software Sicherheitslücken?

Um **System-Lücken** in Windows-Systemen zu schließen, bedarf es zunächst einer regelmäßigen Aktualisierung durch Windows-Updates: http://update.microsoft.com

Der Angriffspunkt Nummer eins im Internet ist der verwendete **Browser**. Der Microsoft Internet Explorer ist aufgrund seiner großen Verbreitung ein beliebtes Ziel für Hacker. Darüber hinaus besitzt er Sicherheitslücken, die nur mit hohem Konfigurationsaufwand und einer gleichzeitigen Einschränkung der Features geschlossen werden können. Eine sinnvolle Alternative ist für viele User der frei erhältliche Mozilla Firefox (http://www.getfirefox.de). Er bietet bei großem Funktionsumfang

ecmc Europäisches Zentrum
für Medienkompetenz GmbH
eMail: info@ecmc.de
Internet: www.ecmc.de
Bergstr. 8 • 45770 Marl
Telefon: +49 (0)2365 9404-0
Fax: +49 (0)2365 9404-29
Zollhof 2a • 40211 Düsseldorf
eMail: info@ecmc.de
Telefon: +49 (0)211 90104-35/-36
Fax: +49 (0)211 90104-37

ecmc

ein zufrieden stellendes Maß an Sicherheit. Einen kostenlosen Sicherheitscheck des von Ihnen verwendeten Browsers bietet der Heise Verlag unter http://www.heise.de/security/dienste/browsercheck an.

Der eMail-Client ist neben dem Browser die zweite große Angriffstelle auf Ihrem Rechner. Insbesondere Programme mit einer automatischen Bildervorschau-Funktion auf externe Bilddateien (wie Outlook und Outlook Express) bieten hier diverse Angriffsmöglichkeiten. Auch die standardmäßig frei geschaltete Nachrichten-Vorschau erlaubt es zum Beispiel Viren und Trojanern, sich sofort im System niederzulassen. Deshalb sollten Sie diese Funktion unbedingt ausschalten! Die automatische Bildanzeige von verlinkten Bildern im Netz birgt eine weitere Gefahr. Freie Systeme wie Mozilla Thunderbird (http://www.thunderbird-mail.de) bieten hier sinnvolle Alternativen.

3. Machen sich Viren, Würmer und Trojaner auf Ihrem PC breit?

Um sich gegen **Spam**-Mails zu wappnen, bedarf es entweder eines in den eMail-Client (z.B. Outlook, Thunderbird, Eudora) integrierten Spam-Filters oder eines speziellen Plugins eines Drittanbieters (z.B. Cloudmark, Spamlook, Alchemy). Hier gibt es je nach Bedarf kostenpflichtige Anwendungen, aber auch freie Software, sogenannte Freeware, am Markt. Es ist sinnvoll, zunächst die Funktionen des internen, kostenlosen Filters Ihres installierten eMail-Clients zu nutzen und diesen bei komplexeren Anforderungen durch ein zusätzliches (evtl. kostenpflichtiges) Plugin zu erweitern. Außerdem bieten die meisten eMail-Provider (wie web.de, GMX oder Hotmail) nicht nur kostenlose eMail-Adressen und Postfächer an, sondern filtern auf Wunsch auch eingehende Spam-Mails aus. Meist arbeiten die Filterprogramme der großen Provider effektiver und werden regelmäßiger aktualisiert als private Software. Generell empfiehlt sich die Benutzung eines Webmail-Accounts - auch wenn Sie einen eigenen eMail-Account auf Ihrem Rechner haben. Die in den Mails versteckten schädlichen Programme und HTML-Elemente können dort als reiner Text angezeigt werden und so keinen Schaden auf dem heimischen Computer anrichten. Ein weiterer Vorteil: Ihre eMails sind weltweit abrufbar. Die bekanntesten Anbieter von Webmail-Accounts sind: web.de, GMX und Hotmail.

Ein **Virenscanner** ist auf jedem System dringend empfohlen. Dieser bietet in der Regel einen sehr umfassenden Schutz des Systems. Auch hier gibt es kostenlose und kommerzielle Lösungen. Man sollte kostenpflichtige Lösungen nicht scheuen, da bei diesen die langfristige Absicherung von aktuellen Virendatenbanken eher gewährleistet ist als bei freien Tools. Empfehlungen sind hier Kaspersky Internet Security das Antivirenkit von GDATA, Symantec AntiVirus 2006 und Antivirus 2007 von Panda Software:

- Kaspersky Antivir — http://www.kaspersky.de
- GData — http://www.gdata.de
- Symantec — http://www.symantec.de
- Panda Software — http://www.panda-software.de

Trojaner und Backdoorprogramme schleichen sich meist unbemerkt über das Herunterladen per Browser ins System oder greifen wahllos im Netz befindliche Rechner an und nutzen Sicherheitslücken im System aus. Sie nisten sich ein und greifen von dort wiederum andere Rechner an. Einen wirksamen Schutz gegen sie bietet eine Firewall.

Neben den Hardware-Firewalls, die in den meisten (DSL-)Routern vorhanden sind, gibt es so genannte Desktop-Firewalls, die dann zum Einsatz kommen sollten, falls man mit dem Rechner direkt ins Netz geht (Modem, ISDN, etc). Sie bieten zwar nicht diese Sicherheit, wie es Hardware-Firewalls können, da sie ein regelmäßiges Eingreifen (Bestätigen/Ablehnen von Datenverkehr) erfordern. Welche Zugriffe

erlaubt, und welche tunlichst untersagt werden müssen, ist für den unerfahrenen User nur schwer einzuschätzen.

Dennoch bieten Desktop-Firewalls den einzigen Schutz beim direkten Kontakt mir dem Internet. Nennenswert sind neben der Software Sygate Personal Firewall, die zur freien Benutzung im Netz zur Verfügung steht, auch Zone Alarm, Tiny Personal Firewall und Norton Personal Firewall:

- Sygate Personal Firewall http://www.sygate.de
- Zonealarm Firewall http://www.zonelabs.com
- Tinysoftware http://www.tinysoftware.com
- Symantec http://www.symantec.de

Dialer nisten sich via Browser im heimischen PC ein. Hier bedarf es einerseits eines wachsamen Auges. Andererseits kann ein Dialer nur dann ansetzen, wenn das System einen direkten Netzzugang per ISDN oder per Modem besitzt. Mit einem DSL-Anschluss oder einem Zugang per Router kann ein Dialer keinen finanziellen Schaden anrichten. Aktuelle Anti-Viren- und Spyware-Programme enthalten in der Regel spezielle Vorrichtungen, um Dialer auf Ihrem System zu erkennen und einen Zugang zu unterbinden. Darüber hinaus finden sich im Netz sehr viele Freewareprogramme, die sich der Dialerproblematik annehmen, wie z.B. der 0190-Warner unter http://www.wt-rate.com. Weitere Informationen über Dialer bieten die Verbraucherzentralen oder:

- http://www.bundesnetzagentur.de
- http://www.dialerschutz.de

Spyware bzw. Adware kann sich per Browser ins System einschleichen, ist aber auch Bestandteil etlicher Free- und Sharewareprogramme. Diese Programme spionieren entweder das Surfverhalten oder Passworte des Users beim Onlineshopping oder Onlinebanking aus. Gegen Spy- und Adware helfen viele freie Tools, die das eigene System auf eben solche Programme untersuchen und diese entfernen. Hier gibt es unter anderem Ad-Aware von Lavasoft, AntiSpyware von Microsoft oder Spybot – „Search and Destroy". Für fortgeschrittene User empfiehlt sich das sehr beliebte und hoch gelobte Programm „HijackThis":

- Lavasoft Ad-Aware http://www.lavasoft.de
- Spybot Search & Destroy http://www.safer-networking.org
- HijackThis: http://www.hijackthis.de

4. Sind Sie auch mobil vernetzt?

Unverschlüsselt über ein **WLAN-Netzwerk** übertragene Daten sind prinzipiell von jeder Person in der Reichweite Ihres Funknetzwerkes lesbar. Übertragen Sie Ihre Daten in einem unverschlüsselten, d.h. ungeschützten WLAN-Netzwerk, könnten Sie ebenso gut Informationen von Ihrem Wohnungsfenster zum Fenster Ihres Nachbarn hinüberrufen und darauf hoffen, dass Ihnen niemand zuhört. Angriffe auf ein lokales Netz erfolgen von einem Angreifer, der das eigene Funk-Netzwerk als quasi neuer Netzuser betritt. Um dies zu verhindern, kann der Zugriff über die jedem WLAN-Gerät eindeutig zugewiesene MAC-Adresse reglementiert werden, indem nur den eigenen Adressen Zugriffe erlaubt werden. Darüber hinaus sollten Sie den Datentransfer mindestens über eine WEP-Verschlüsselung absichern, besser noch durch die etwas neuere und sicherere WPA-Verschlüsselung. Beide Schutzmechanismen werden in den Handbüchern der WLAN-Endgeräte beschrieben und sind unter den Stichworten „MAC-Adresse" und „WEP-Verschlüsselung" respektive „WPA-Verschlüsselung" zu finden.

Bluetooth wird vorwiegend bei Handys und PDAs zur Kopplung mit anderen elektronischen Geräten benutzt. Dabei existiert die Gefahr der Übernahme Ihrer persönlichen Daten durch Fremde. Hier gilt eine einfache Regel zu Ihrer Sicherheit:

Wenn Sie diese Technologie nicht ausdrücklich benötigen, schalten Sie sie ab – gerade in öffentlichen Bereichen wie Bahnhöfen oder Flugplätzen.

5. Sind Sie bereit, für Inhalte im Internet zu zahlen?

In den vergangenen Monaten haben es die Verbreiter unseriöser Internetangebote zunehmend auf Kinder und Jugendliche abgesehen. Online-Hausaufgabendienste, Landkarten-Services und Spieleseiten locken häufig mit so genannten Premiumdiensten. Diese sind fast immer mit (relativ hohen) Zahlungen verbunden und bieten oft weniger Informationen als freie Internetangebote.

6. Alle Links im Überblick:

Microsoft Updates	http://update.microsoft.com
Mozilla Firefox Browser	http://www.getfirefox.de
Heise Browsercheck	http://www.heise.de/security/dienste
Mozilla Thunderbird	http://www.thunderbird-mail.de/
Kaspersky Antivir Demo	http://www.heise.de/security/dienste/antivirus
Kaspersky Antivir	http://www.kaspersky.de
GData	http://www.gdata.de
Symantec	http://www.symantec.de
Panda Software	http://www.panda-software.de
Sygate Personal Firewall	http://www.sygate.de
Zonealarm Firewall	http://www.zonelabs.com
Tinysoftware	http://www.tinysoftware.com
Symantec	http://www.symantec.de
0190-Warner	http://www.wt-rate.com
Lavasoft Ad-Aware	http://www.lavasoft.de
Spybot Search and Destroy	http://www.safer-networking.org
HijackThis:	http://www.hijackthis.de
Password Gorilla	http://www.fpx.de/fp/Software/Gorilla
Passwort.Tresor	http://www.passworttresor.de/download.php3
Passwort Generator	http://www.atory.com/Password_Generator/