

## Sicherheit im Internet – sicher ist sicher

Gehören auch Sie zu den etwas verunsicherten Durchschnitts-Normalanwendern von Computern, die in letzter Zeit vermehrt bei zufällig erlauchten „Geschichtln“ so mancher Experten von den Reizwörtern „Hacker“, „Viren“ und „Spam“ aufgeschreckt werden oder gar jenen, die sich kaum der den eigenen Computer einschalten getrauen, da Sie befürchten die Internet-Hacker könnten in Ihren PC einbrechen? Wir wollen Ihnen in dieser Folge das Thema „Computersicherheit“ näherbringen und dabei helfen dieses Problem besser abschätzen und damit vielleicht auch ein bisschen besser schlafen zu können – auch während Ihr PC läuft.

### **„Hacker“ – wer fummelt da auf meinem Rechner herum?**

Wenn Sie einen PC mit Internetanschluss betreiben, gibt es zumindest eine theoretische Möglichkeit für andere, auf Ihren PC zuzugreifen – je nachdem wie gut oder schlecht Ihr Gerät geschützt ist. Umgangssprachlich hat sich der Begriff des „Hackers“ eingebürgert, das sind Leute, die sich nächtelang (wahrscheinlich in verqualmten Kellern der Bronx) nur damit beschäftigen, in fremde Computersysteme einzudringen. Die Literatur zu diesem Thema füllt Regale und im Wochentakt werden neue Angriffsmöglichkeiten publiziert, die es ermöglichen

**Router** ... Netzwerkgerät zur Vermittlung von Datenpaketen im Internet oder Heimnetzwerk

**Wurm** ... schädliche Programme, die Sicherheitslücken in Software nutzen, um sich auf Rechnern im Internet zu verbreiten. Der legendäre „Blaster“-Wurm kann ältere Windows-Betriebssysteme befehlen und sich damit weiterverbreiten.

**Viren** ... in Bezug auf Computer ein schädliche Softwarefragmente, die sich meist via E-Mail verbreiten.

**Download** ... „Herunterladen“ von Dateien aus dem Internet auf den eigenen Computer

**Update** ... Aktualisierungen des Betriebssystems, von Software oder Virenschutzprogrammen aus dem Internet

vor allem die gängigen Windows-Betriebssysteme einzubrechen. Wie können Sie sich nun schützen? Der wirksamste Schutz ist hier sicher eine Hardwarelösung – sprich ein sogenannter „Router“, über den der ganze Internetverkehr läuft. So ein Gerät bekommen Sie beispielsweise bei einem ADSL-Anschluss der Telekom mitgeliefert und standardmäßig „zugemacht“ – d.h. keine Zugangsmöglichkeit von außen. Wenn Sie direkt am Internetanschluss „hängen“ wie das z.B. bei Chello üblich ist, müssen Sie selbst vorsorgen – sprich eine sogenannte „Firewall“ installieren. Diese Firewall haben Sie beim neuen Windows XP (wichtig: „Service Pack 2“) gleich dabei, bei älteren Windows Versionen müssen Sie höllisch aufpassen, da schon während der Installation Ihr System (durch sogenannte Würmer) innerhalb

von Sekunden attackiert werden kann. Das ganze läuft vorläufig völlig unbemerkt – daher in diesem Fall unbedingt den Netzwerkanschluss erst dann vornehmen, wenn die Firewall läuft.

Wenn Sie auf obengenannte Maßnahmen verzichten, sollten Sie eher schlecht schlafen, da es Möglichkeiten für Angriffe aus dem Internet gibt. Also – wenn kein Router vorhanden ist bitte unbedingt eine Firewall installieren (z.B. „Zone Alarm“ unter <http://www.zonealarm.com/> zu beziehen). Virenschutzprogramme sind zwar in der Lage, bekannte Würmer zu finden und zu deaktivieren, können aber keine manuellen Attacken auf Ihren PC verhindern – deshalb die Firewall. Zusätzlichen Schutz haben Sie jedenfalls durch ständige Aktualisierungen Ihres Betriebssystems (automatische Updates) aus dem Internet. Diese Updates stopfen die laufend bekannt werdenden Sicherheitslöcher durch Installation sogenannter „Patches“, die kleine oder größere Schlampigkeiten der Entwickler von Betriebssystemen im Nachhinein ausbügeln sollen.

## **Wenn Computer erkranken**

Computerviren haben seit den 70er Jahren die Entwicklung des Computers begleitet, wer erinnert sich noch an den „Keks“-Virus, der nur verlangte, dass die Benutzer das Wort „KEKS“ auf die Bitte nach der Süßigkeit eingeben. Die Verbreitung erfolgte zuerst über Disketten, mit der rasanten Vernetzung der Rechner via Internet ist heute E-Mail in fataler Verbindung mit ungesicherten Betriebssystemen das willigste Transportmedium. Um das Eindringen von Computerviren in Ihren PC zu verhindern, sollten Sie grundsätzlich keine Dateianhänge öffnen, die „komische“ Dateieendungen aufweisen („com“, „pif“, etc.). Sie brauchen unabhängig davon jedenfalls ein Virenschutzprogramm, das stets aktuell sein muss (Updates aus dem Internet müssen automatisch erfolgen) – verlängern Sie daher immer das Abonnement. Bedenken Sie, dass Computerviren ganz schöne Schäden auf Ihrem Rechner verursachen können – bis zum Löschen wichtiger Daten (für die es meistens keine Sicherung gibt). Aktuelle Computerviren sind auch schon so „ausgereift“, dass Sie gleich weitere Lücken in Ihrem System öffnen, Virenschutzprogramme beenden, selbsttätig E-Mails zur Weiterverbreitung an Empfänger Ihres Adressbuchs verschicken, etc. etc.

Wir haben heute einmal die wichtigsten Fragen zum Schutz Ihres PCs besprochen, in der nächsten Folge soll es um Fragen des Datenschutzes gehen, d.h. um kleine Programme, die Ihr Surfverhalten messen oder Sie beim Arbeiten belästigen („spam“ und „spyware“).

Für Detailfragen senden Sie bitte Ihre E-Mail an:

**Müller & Kanduth OEG**  
**support@mko.at**