



Internet

Beitrag zum Thema «Gute Vorsätze für das neue Jahr»

Auch 2006 gilt: Schütze sich, wer kann!

So mancher Surfer holt sich mit scheinbar harmloser Software oder beim Besuch von Webseiten mit aktiven Inhalten ungebundene Besucher auf seinen PC. Aber wer will sich schon sein Postfach mit dem ewigen Rolex-Quatsch oder irgendeiner Potenzhilfe zumüllen lassen. Nahezu alle Massnahmen, die der Computersicherheit dienen, gehen mit einem Verzicht auf Bequemlichkeit einher. Sicherheit beginnt daher in den Köpfen der Anwender. Solange sie Passwörter abspeichern, um sie nicht jedesmal neu eingeben zu müssen, veraltete Software mit bekannten Sicherheitsmängeln einsetzen und ihre Browser so konfigurieren, dass lästige Sicherheitshinweise unterbleiben, sind sie leichte Beute für Datenspione und -saboteure. Hier zuerst mal einige grundsätzliche Sicherheitsvorkehrungen und ein paar nützliche – und erst noch kostenlose – Tools für mehr Sicherheit auf dem Web.

Allen Leserinnen und Lesern wünsche ich nachträglich noch es guets Neus!

Thomas Vauthier
th.vauthier@bluewin.ch

Security-Update: Schutz der eigenen Privatsphäre

Die Bedrohung wächst – so stark wie selten zuvor. Das belegen aktuelle Studien. Betroffen durch Betrug, Hacking und Sicherheitslöcher sind nicht nur Unternehmen, sondern ebenso Privatpersonen. Höchste Zeit auch für jeden Privatanwender, sich um seine Privatsphäre auf dem vernetzten Computer zu sorgen und Abhilfe gegen die vielfältigen Angriffsformen zu schaffen.

Dabei beginnt der Schutz der eigenen Umgebung bei der Frage des Zugriffs auf den eigenen Computer. *Deskman Professional* sichert nach wenigen Mausklicks auf der schönen Benutzeroberfläche den kompletten Desktop ab und sorgt dafür, dass nur legitimierte Personen bestimmte Programme oder Ordner nutzen können. Damit bleiben einem auch unliebsame Verstellungen im System oder auf dem Desktop erspart, obwohl sich (auch dank der Benutzerprofile) weiterhin mehrere Personen den PC teilen können. Wer kein Geld ausgeben will, kann zu dem in der Grundversion kostenlosen *WinGuard Pro Free* greifen, um einen

vergleichbaren Schutz zu erreichen – wenn auch mit einer spartanischeren Oberfläche, so doch ebenfalls sicher.

Möchte man nicht so weit gehen und den ganzen PC mit einem Schutzsystem für jeden Winkel absichern, so kann man mittels Folder Guard Standard gezielt einzelne Ordner vor Neugierigen verstecken. Die mit Hilfe dieses Tools manipulierten Verzeichnisse sind weder unter DOS noch unter Windows aufzuspüren und lassen sich auch nicht in einem Dateimanager oder einer Programmdateibox sichtbar machen.

Spam vorbeugen

Geben Sie Ihre E-Mail-Adresse nur Personen, die Sie kennen und/oder denen Sie vertrauen. Verwenden Sie eine E-Mail-Adresse für den privaten Mailverkehr und eine zweite Adresse für alle sonstigen Web-Aktivitäten.

Mindestausrüstung: Firewall, Antivirus, Anti-Spyware

Um beim Arbeiten die grössten Gefahren aus dem Internet abzublocken, empfiehlt sich dringend die Einrichtung einer persönlichen Firewall wie z.B. der *Tiny Personal Firewall*. Durch die Kombination von Sandbox-Technologie und der Paketprüfung aller Internetkommunikation wird ein Höchstmass an Schutz vor Spionage und Hackerattacken in allen Bereichen der täglichen Internetnutzung erreicht. Mit kleinen Tools wie *LeakTest* kann man bei Interesse die Arbeitsweise von Personal Firewalls überprüfen.

Und auch wenn durch die Firewalls die Datenströme kontrolliert werden, ist darüber hinaus ein Antivirusprogramm unerlässlich: *AntiVir Personal Edition* wird als kostenloser Virens Scanner mehrfach wöchentlich aktualisiert und sorgt so dafür, dass mehr als 60 000 Virenarten in Dateien und Programmen abgefangen werden, indem es mit dem Virenwächter permanent achtsam ist oder gezielt auf die Suche geschickt wird. Der sorgsame Umgang z.B. mit Mails ist zwar weiterhin wichtig, aber die Unterstützung durch permanente Weiterentwicklung bildet eigene gute Vertrauensbasis.

Besonderer Beachtung bedürfen die so genannten Trojaner, die in ein System eingeschleust werden, um unbemerkt Daten und Aktivitäten auszuspionieren. Mittels Anti-Trojan kann man ganz gezielt nach solchen Trojanern spüren und sie eliminieren oder mit Tools wie *Klez & Elkern Removal Tool* gezielt anderes Getier wie Würmer ausmerzen.

Eine andere Möglichkeit, ausspioniert zu werden, ist durch so genannte Spyware, die die Nutzeraktivitäten vor allem im Web nachzeichnet und sammelt. Schutz vor solch dubiosen Spionageangriffen bietet z.B. das kostenlose Tool *Spybot – Search & Destroy*.

Hat man schliesslich seine Arbeit am Computer beendet, so findet ein Dritter mit blossen Auge viele der eigenen Aktivitäten aufgezeichnet in Verlauffliste, History, Logdateien etc. – vor allem alle Handlungen im Web. Mit etwas Vorbereitung lässt sich das vermeiden. Z.B. löscht *Steganos*-Internetspurenvernichter sämtliche dieser Listen und Historien. Noch weiter geht *AbsoluteShield Internet Eraser Pro*, indem das Tool auch Spuren aller anderen Aktivitäten auf dem PC löschen kann. Damit sind die eigenen Handlungen nicht mehr nachvollziehbar, und die eigene Privatsphäre bleibt gewahrt.

Fazit

Ohne eine eigene IT-Abteilung oder Antivirus- und Firewall-Lösungen auf dem Server sind Praxen und Privatanwender auf einen eigenen Schutz vor Hackern und anderen Bedrohungen aus dem Internet angewiesen. Ausser den hier zusammengefassten Schutzmassnahmen bringen «Sicherheitsuiten» alles mit, was man benötigt, vom Antiviruschutz über Firewall bis hin zum Datenschutz im Internet – alles in einem Paket.

Davon mehr im nächsten Beitrag.

