Technische Grundlagen für Eltern

Ausgangslage

Diese Tipps sind für Privathaushalte mit bis zu 5 PCs gedacht, die über einen DSL-Anschluss mit einem oder mehreren Telefonanschlüssen verfügen. Die Anlage besteht normalerweise aus Splitter, DSL-Modem, Router mit eingebauter Hardware-Firewall und angeschlossenen PCs.

Selbstverständlichkeiten

Die **Firewall**-Funktion Ihres Routers muss durch ein Passwort abgesichert sein, das Sie selbst setzen (NIE die Voreinstellung einfach lassen, wie sie ist). *Jeder* Ihrer Computer muss über einen **Virenschutz** (*nicht* kostenlos!) verfügen. Empfehlung: keine „Suite“ sondern ein reines Anti-Virus-Programm verwenden. Unter Windows muss die Windows-Firewall aktiviert sein. Automatische Updates sollten eingeschaltet sein.

Verträge

Sie sollten eine „echte Flatrate“ verwenden. Das bedeutet:

- keine Zeitbegrenzung, keine Volumenbegrenzung fürs Internet
- Kostenloses, zeitlich unbegrenztes Telefonieren ins deutsche Festnetz

Sie sollten kostenpflichtige, werbefreie E-Mail-Accounts verwenden, die eingehende Mails automatisch von einem Großteil der Schädlinge (Viren, SPAM und Phishing) befreien. Das erzeugt geringe Kosten, bringt jedoch einen gewaltigen Gewinn an Sicherheit und Privatsphäre.

Lizenzen

Jeder PC sollte korrekt lizenziert sein. Eine legale Windows-Lizenz bedeutet tatsächlich ein Mehr an Sicherheit, ebenso wie ein Lizenz-Bruch ein Sicherheitsrisiko darstellt. FREIE Lizenzformen (FreeWare, OpenSource, ShareWare) können einem Privathaushalt hier viel Geld sparen (Beispiel: Open Office; Linux; Thunderbird) und eröffnen Ihrem Schulkind eine ganze Welt des Lernens und Ausprobierens, die sehr sicher *und* legal ist *und* nichts kostet.

Benutzer-Rechte

Die Benutzer-Rechte der Computeranlage sollten in Familien ebenso wie in Firmen nach Verantwortung gestaffelt sein, und zwar deshalb, weil der Verantwortliche vor Gericht haftet. Die elterliche Aufsichtspflicht müssen Eltern eben auch praktisch wahrnehmen können. Daher sollte Ihr Kind nur Benutzer-Rechte am Computer, nicht aber Administratorrechte haben. Diese Maßnahme schützt Ihre Familie vor unerlaubten Programmen, etlichen Computerviren und vor vielen teuren Installationskosten.

Passwörter

Sichere Passwörter werden am einfachsten erzeugt, indem Sie die Anfangsbuchstaben eines Zitats oder eines Spruches, der Ihnen besonders gefällt, zu einem Wort zusammensetzen und willkürlich noch Zahlen hinzufügen. Beispiel: „**D**as **I**st **A**lles **N**ur **G**eklaut“ und die letzte Zahl des aktuellen

Jahres (201**0)** könnte man zu folgendem leicht zu merkenden Passwort zusammensetzen: DIANG0, Merkhilfe: Django. Um wirklich sicher zu sein, sollte Ihr Passwort allerdings mehr als sechs Stellen haben. Bitte verwenden Sie NIE Namen Ihrer Angehörigen, Freunde und Haustiere, Geburtsdaten oder Allgemeinbegriffe als Passwort. Zeichenketten, die auch im Lexikon vorkommen, sind ungeeignet.

Datensicherung

Alle privaten und beruflichen Daten müssen gesichert werden. Sie sollten mehrere externe Datenträger besitzen und verwenden: externe Festplatten, USB-Sticks oder Speicherkarten. Daten, die Sie nur auf einem einzigen Datenträger abspeichern – der eingebauten Festplatte Ihres Computers, zum Beispiel – *werden unrettbar zerstört* werden. Die Frage ist nur, wann.

Vertiefungshinweis:

Benutzen Sie (unter Windows) die Funktion „Wiederherstellungspunkt“. Sie können außerdem die gesamte Installation Ihres Computersystems SICHERN, wenn Sie sie erst einmal fertig eingerichtet haben und alles funktioniert. Das ist ein guter Weg, sich viel Arbeit zu sparen. Die Installation von Zeit zu Zeit wieder „zurückzusetzen“, ist außerdem ein guter Schutz gegen Hacker und viele Viren. Eine Sicherung einer kompletten Festplatte nennt man ein „Image“.

Drahtloses Internet

Drahtlose Verbindungen (WLan) sind kompliziert einzurichten und unsicher. Empfehlung: schließen Sie Ihre diversen Computer über Netzwerk-Kabel („Patchkabel“) ans Internet an. Um Ihr Internet im ganzen Haus verfügbar zu machen, können Sie das Signal von Steckdose zu Steckdose weiterleiten. Ein Hauptvorteil dabei ist, dass Sie vor Missbrauch durch Dritte sicher sind – und, dass Sie die Internet-Nutzung in Ihrem Haushalt kontrollieren können.

Falls Sie WLan zu Hause haben wollen, sollten Sie WPA2 einsetzen, sichere Passwörter verwenden, die Fernkonfiguration ausschalten, eine neutrale SSID verwenden, die keine Rückschlüsse auf Standort, Geräte oder Verwender zulässt, regelmäßig Firmware-Updates durchführen, die Passphrase (Pre-Shared-Key) sollte die maximale Schlüssellänge auch wirklich ausnutzen (63 Zeichen), und Sie sollten das Gerät ausschalten, wenn es nicht genutzt wird.

Sie können für Schäden, die dadurch entstehen, dass Unbekannte in Ihr WLan einbrechen, unter Umständen haftbar gemacht werden.

Problem-Bewusstsein

Computer sind nicht unfehlbar, elektronische Geräte gehen leicht kaputt, Jugendliche sind leichtfertig und das Internet ist voll von übelsten Berufs-Abzockern, die das Rechtssystem gegen Sie ausspielen. Sich das bewusst zu machen und entsprechende Vorsicht anzuwenden, verschafft Ihnen bereits deutlich mehr Sicherheit.

Verantwortlich für dieses Infoblatt, V.i.S.d.P., Kontakt:

Timmo Strohm
Allgäustr. 2
88212 Ravensburg
Tel. 0751 / 3550-378
E-Mail: timmo.strohm@gmx.de