Wie sichere ich mich und meinen Rechner?

Dies ist eine Zusammenfassung von 11 Möglichkeiten Ihres eigenen Schutzes, die früher zeitaufwändig und daher sehr lästig waren. Die Möglichkeiten kosten Geld, meist nicht viel, doch sie werden Ihnen helfen.

1. Installieren Sie eine Antivirensoftware

Die bekannten Antiviren-Programme bieten alle ein hohes Schutzniveau in allen Bereichen Ihres Rechners. Sie schützen vor Attacken aus dem Web, von E-Mails oder aus den USB-Sticks. Dabei reicht eine kostenlosen Antiviren-Suite. Avast oder Avira als Freeware sind nicht schlecht, beinhalten aber jede Menge Werbung. Der Windows Defender ist besser als nichts, bietet aber ein geringes Schutzniveau. Einmal installiert, kann sich Antivirensoftware selbst updaten und Ihren Rechner stets überwachen.

2. Sichern Sie Ihre Daten regelmäßig per Backup

Die langweiligste, aber letztendlich wichtigste Regel für die Sicherheit Ihrer Daten ist das Backup. Sie können sich nie hundertprozentig vor Trojanern und Festplattenzusammenbrüchen schützen. Mit einem Backup gehen Ihre Daten dann nicht verloren. Sind Ihnen die Daten wichtig, dann sichern Sie diese mindestens täglich, und zwar auf ein Medium, das Sie vom Computer entnehmen können, oder das im Netzwerk existiert. Weil Sie natürlich **nicht** immer daran denken, die Daten zu sichern, verwenden Sie eine Software, die das automatisch für Sie erledigt. (z.B. Ashampoo Backup)

3. Halten Sie Ihre Software Up-to-Date

Da heute fast alle Programme mit dem Internet verbunden sind, haben auch alle auch Sicherheitslücken. Diese werden nur durch Updates behoben. Dabei ist ein aktuelles Betriebssystem, gefolgt von allen Internetprogrammen und auch Browser-Plugins wie Flash und Java und natürlich die Antivirensoftware am wichtigsten. Sinnvoll ist es, die Updates immer automatisch ablaufen zu lassen.

4. Verwenden Sie immer sichere Passwörter

Je wichtiger Ihnen Ihre Daten sind, desto sicherer sollte Ihr Passwort sein. Doch was ist ein sicheres Passwort? Es sollte mind. 12 Zeichen mit Ziffern und Sonderzeichen beinhalten und keine, keine sprachlichen Begriffe enthalten. Jede Anwendung sollte ein eigenes Passwort erhalten. Dann haben Sie natürlich Probleme, sich Ihre Passwörter zu merken. Nehmen Sie dazu einen Passwortmanager wie z.B. Keepass.

5. Verwenden Sie WINDOWS nur als Anwender

In WINDOWS sollten Sie nie als Administrator arbeiten oder gar surfen. Legen Sie von Anfang an einen einfachen Account an und gewöhnen Sie sich daran, mit diesem im Alltag zu arbeiten.

6. Vorsicht bei Browser-Skripten und -Plugins

Das Haupteinfallstor für Schädlinge ist das Web. Bösartige Seiten (oder bösartige Banner auf gutartigen Seiten) installieren Trojaner über Lücken in Browsern und dessen Plugins. Updates verringern zwar deren schädliche Auswirkungen, reichen aber nicht. Es ist zusätzlich sinnvoll, Skripte einzuschränken. Hier hat sich z.B. das Firefox-Add-on "**NoScript**" bewährt. Sehen Sie dann nur weiße Seiten? Einmal müssen Sie das Tool einstellen. Deaktivieren Sie so viele Plugins wie möglich (insbesondere Java) und stellen Sie die anderen auf Nachfragen, wenn aktiviert werden soll.

7. Seien Sie vorsichtig mit fremden Geräten. Jeder USB-Stick/jedes USB-Laufwerk kann Viren und Trojaner auf Ihren Rechner übertragen. Schließen Sie also nicht jeden Stick an, der in Ihre Hände gelangt. Seien Sie vorsichtig mit Fotoautomaten, auf Messen oder in Ihrer privaten Umgebung. Zwar hilft Ihnen Ihre Antiviren-Software, doch die kennt vielleicht auch nicht nicht jeden Virus und täglich werden Hunderte neue entwickelt.

8. Seien Sie sehr kritisch mit fremden Daten

Fremde Daten müssen Sie nicht willentlich mit Viren überschütten, doch würde ich nie den Stick meines computerspielbesessenen Sohnes zu Datenverteilung nutzen. Da hilft auch Formatieren nichts. Bei ausführbaren Dateien ist die Möglichkeit der Virenübertragung am größten. Zu den ausführbaren Dateien gehören nicht nur *.exe-Dateien, sondern besonders auch Macros, die als Dateianhänge mit Office-Dokumenten zu Ihnen ins Haus gekommen sein können. Seit der MS-Office-Version 2007 startet MS-Office keine Makros mehr automatisch. Oben im Office-Produkt ist ein Balken mit der Nachricht zum aktivieren der Inhalte eingeblendet. Ein weiterer Ort zur Verteilung von Viren sind die Video-Kodizes. So ein Codecs, den man für Internetvideos nachladen soll, ist ein beliebter Hacker-Trick bei Virenerzeugern. Oft steckt ein Trojaner in so einem Codecs.

9. Sichern Sie sich gegen E-Mail Betrug

Ihre geheimsten Daten, z.B. für Chipkarten, zu ergattern, kann einen Betrüger reich machen. Betrüger versenden E-Mails, die es auf Ihre Daten und Ihr Geld abgesehen haben. Gute Email-Programme und Browser warnen Sie über solche Phishing-Versuche.

10. Sichern Sie Ihren Router gegen Hackerangriffe ab

Ihr Router ist der zentrale Angriffspunkt auf Ihr Heimnetz. Hat sich ein Angreifer hier festgesetzt, kann er weitgehend unbemerkt Ihr Netz und alle Geräte kontrollieren. Sie sollten den Router besonders gut schützen. Das fängt bei einem sehr sicheren Passwort für die Weboberfläche an (20 zufällige Zeichen, z.B. mit Keepass erzeugt) und endet bei Updates für die Firmware. Gerade in dicht besiedelten Gebieten sollten Sie auch für Ihr WLAN einen sicheren und langen Schlüssel nehmen und diesen regelmäßig wechseln. Wählen Sie als Verschlüsselungsstandard für das Funknetz WPA2 (CCMP), keinen anderen. Jeder Dienst des Routers (z.B: Fernzugriff auf Router oder NAS) stellt ein Risiko dar. Öffnen Sie so wenig Ports wie möglich in der Router-Firewall, denn jeder offene Port ist ein Einfallstor in Ihr komplettes Heimnetz.

11. Seien Sie vorsichtig in fremden Netzen

Wenn Sie mit Ihrem Laptop Teil eines fremden, möglicherweise sogar offenen WLANs werden, sind Sie in besonderer Gefahr. Sie befinden sich mit allen Rechnern auf diese Art und Weise zugreifenden Rechnern im gleichen Netz, sodass viele Sicherheitsmechanismen nicht greifen. Im WINDOWS-Netz wählen Sie unbedingt „Gast“ oder „Öffentliches Netz“ und prüfen Sie das in den Netzwerkeinstellungen. Dort sollten Sie auch unbedingt die Datei- und Druckerfreigabe deaktivieren. Zusätzlich sollten Sie nur mit VPN surfen (z.B. „Avira Phantom“, „Spyoff“ oder „Okay Freedom“). Das verhindert spezielle Angriffe auf Logins und schützt Sie gleichzeitig vor dem neugierigen Betreiber des Hotspots, über dessen Router ja alle Daten fließen.

Krähenberg – Verlag

Dieser Artikel wurde Ihnen präsentiert von Dipl.-Ing. (FH) Stefan Leybold,

Krähenberg – Verlag

Verlag, Administration, Schulungen und Shop

für das CAD - Institute