

Tipps mit denen Sie Ihren PC sicherer machen können!

Die Gefahren

Auch wenn Sie es nicht merken, jedes Mal, wenn Sie surfen lassen sie im Internet digitale Fußspuren zurück. Auf vielen Webseiten werden Logfiles erstellt, Ihre Daten gesammelt und, wenn Sie Pech haben, zu Werbezwecken weiterverkauft. Es ist für Firmen heutzutage sehr einfach, E-Mail-Adressen, Kreditkartennummer und bestellte Waren einander zuzuordnen und so ein genaues Benutzerprofil zu erstellen.

Auch ihre E-Mails sind für Hacker oder Geheimdienste leicht lesbar. So werden z.B. alle digitalen Nachrichten (Handygespräche, Faxe, E-Mails usw.) vom Spionagenetz Echolon gespeichert und nach bestimmten Stichworten durchsucht. Das Echolon wird u.a. vom Geheimdienst der USA betrieben und es gilt als bewiesen, dass der Geheimdienst diese Daten z.B. zur Wirtschaftsspionage verwendet hat. Sollte Ihre E-Mail also z.B. diverse Wörter beinhalten die auf eine „Gefahr“ hinweisen, würde sie vom Echolonsystem zu einem Geheimdienstmitarbeiter weitergeschickt der sie liest und dann ggf. weitere Schritte einleitet.


Viren kommen heutzutage nicht mehr nur von Disketten. Sie kommen durch Löcher in ihrem Betriebssystem, sie verschicken sich automatisch an Ihre Freunde und sog. Trojanische Pferde können ihren PC ausspionieren und oder ihren PC für Hackerangriffe zweckentfremden ohne das Sie es merken.

Hier haben ich ein paar einfache Tipps zusammen gestellt, mit denen Sie ihren PC sicherer machen können:

Sicherheits-Tipps

1. Passwörter

Hier gilt, je länger ein Passwort ist, desto schwieriger ist es zu knacken. Verwenden Sie eine Kombination von Zahlen und Buchstaben und vermeiden Sie Passwörter, die leicht mit Ihnen in Verbindung gebracht werden können (Name der Ehefrau, Hochzeitstag etc.). Ideal sind Wörter die nicht in einem Wörterbuch o.ä. zu finden sind. Verwenden sie nicht die gleichen Passwörter für mehrere Zwecke, auch wenn es verlockend ist und notieren sie diese nicht auf Zetteln, die von Fremden gefunden werden können.

 **Tipp:** Bilden Sie einen leichten Satz den sie sich gut merken können und nehmen Sie den ersten Buchstaben jedes Wortes.


Beispiel: Mein Kater heißt Francis und ist 8 Jahre alt.


Passwort: MkhFui8Ja


Ihrer Fantasie sind dabei natürlich keine Grenzen gesetzt und so brauchen Sie sich kein kompliziertes Passwort sondern nur einen leichten Satz zu merken!

2. Browser

Der Internet Explorer ist schon seit langer Zeit Ziel der Hacker die sich durch Sicherheitslücken Zugang zu Ihrem Rechner verschaffen und Hintertüren öffnen können. Erst seit kurzem sind viele Nutzer auf Browser wie Opera und Firefox als Alternative zum Internet Explorer aufmerksam geworden und steigen auf die sichere Alternativsoftware um. Besonders Firefox ist sehr attraktiv für viele, nicht zuletzt weil er kostenlos nutzbar ist und ständig durch freiwillige Programmierer weiterentwickelt und verbessert wird. Aber auch wenn Sie nicht auf einen anderen Browser umsteigen wollen, sollten Sie ein paar kleine Tipps berücksichtigen um ihren Browser ein klein wenig sicherer zu machen.

 Internet Explorer Updates: Genauso wie für Windows Betriebssystem (siehe Punkt 7) sollten Sie über das Windows Update die aktuellsten Patches herunterladen und installieren.

 Einstellungen: Achten Sie hier auf die Sicherheitseinstellungen Ihrer Software. Stellen sie beim Internet Explorer ActiveX Komponenten aus, wenn sie auf Nummer sicher gehen wollen. Gleiches gilt eigentlich für Java, doch benutzen zu viele Seiten Java-Elemente.

 Spuren beseitigen: Löschen Sie regelmäßig sowohl den Cache, als auch die History ihres Browsers. Mit nur wenig Mühe kann sonst jeder feststellen, welche Seiten Sie besucht haben.
Internet Explorer: Extras – Internetoptionen – Temporäre Internetdateien
Firefox: Extras – Einstellungen – Datenschutz – Chronik/Cookies/Cache

3. E-Mails

Öffnen Sie niemals Anhänge von Dateien, bevor Sie diese mit einem Virens scanner getestet haben. Selbst wenn sie von einer bekannten Person kommt, können hier Viren versteckt sein. Viele Viren verschicken sich automatisch an alle Einträge im Adressbuch eines E-Mailprogrammes und fälschen die Absenderadresse.

Prüfen Sie, ob Sie E-Mails mit ihrem bevorzugten Mailprogramm verschlüsseln können. Standard ist hier das etwas komplizierte Programm Pretty Good Privacy (PGP), das es in einer kostenlosen Version im Internet gibt (www.pgp.com). Aber viele Mailprogrammen bieten einfachere eingebaute Methoden zur Verschlüsselung.

4. Downloads

Benutzen Sie immer einen Virens scanner zur Überprüfung von heruntergeladenen Daten. Da jede Woche Unmengen neuer Viren erscheinen sollten Sie Ihre Antivirensoftware immer auf dem neusten Stand halten. Nehmen sie möglichst ein Produkt, bei dem Sie jederzeit Zugriff auf Updates haben.

5. Virens scanner

Sie sollten sichergehen das Ihre Virens scanner immer auf dem neusten Stand bleibt und mindestens alle 1-2 Wochen ein Update der Signaturdaten herunterladen. Nur so können Sie sicher sein das Ihr Virens scanner auch aktuelle Viren erkennt und beseitigt. Ein für Privatanwender kostenloser Virens scanner ist Avir Personal Edition (den passenden Link finden Sie am Ende der Seite).

6. Firewalls

Eine Firewall kann Programmen und Daten den Zugang vom und zum Internet erlauben oder verwehren. So kann ein Eindringen von Hackern oder das versenden vertraulicher Daten verhindert werden. Doch nützt so ein Produkt nur richtig, wenn es auch wirklich gut eingestellt ist. Ein einfaches „Ja“ oder „Nein“ für ein Programm nützt wenig weil es einfach auszutricksen ist. Hierfür sollten Sie die Hilfe eines Profis nutzen oder sich genauer mit der Materie befassen. Eine erste und einfache Hilfe ist die in Windows XP integrierte Firewall. Starten Sie dafür das Sicherheitscenter von Windows XP und aktivieren Sie die Firewall. Hier können Sie auch die Einstellungen für die automatischen Windows-Updates einstellen.


7. Windows

Halten Sie ihr Betriebssystem immer auf dem neusten Stand und aktualisieren Sie es durch das Windows Update. Stellen Sie das Update auf automatisch ein, dann brauchen Sie sich in der Regel nicht weiter um die Aktualisierungen zu kümmern. Updates werden dann automatisch heruntergeladen und installiert wenn Sie online sind.

8. Halber Schutz ist besser als keiner

Einige Windowseinstellungen scheinen einen Schutz des PCs zu versprechen, sind jedoch ohne große Probleme und Aufwand zu umgehen.

 **Bildschirmschoner:** Auch wenn Sie ihren Screensaver mit Passwort versehen haben, mit einem Neustart des Rechners kann dieser einfach umgangen werden.

 **Ihre WinWord, Excel-, Accessdateien** können Sie ganz einfach mit Passwort versehen (Datei – Speichern unter – Optionen). Aber auch hier gilt, dass für einen versierten Computerfachmann oder durch einfache Hackersoftware die leicht im Netz zu finden ist, dieser Passwortschutz einfach zu umgehen ist.

9. Ganz einfache Tricks

Verstecken Sie Ordner und Dateien mit dem Windows Explorer vor neugierigen Blicken. (Markieren sie die gewünschte Datei - rechter Mausklick – Eigenschaften – Dateiattribute – Versteckt). Gleichzeitig sollten sie in den Einstellungen des Explorers einstellen, dass versteckte Dateien nicht angezeigt werden

Arbeitsplatz o. Windows Explorer: Extras – Ordneroptionen - Ansicht – Versteckte und Systemdateien ausblenden

Dies ist kein direkter Schutz, sondern dient eher dazu Kinder oder Kollegen vom Löschen oder stöbern in Ihren Dateien abzuhalten.

Aber Sie sehen, selbst mit ein paar einfachen Klicks können sie ihren PC etwas sicherer machen.

Dirk Hagemann

Links zu kostenloser Sicherheits-Software

- ★ Antivir Personal Edition: www.free-av.de
- ★ Firefox Browser: www.firefox-browser.de
- ★ Opera Browser: www.opera.com/lang/de
- ★ KeePass Homepage: keepass.sourceforge.net