Ing. Schönberg Christian

Einzelpreis: kostenlos

Softwareentwicklung

SCHÖNBERG
Softwareentwicklung

http://schoenberg.company

Ing. SCHÖNBERG Christian *
Softwareentwicklung

Schallermühle 6/5,

A-4844 Regau

christian@schoenberg.co.at

**) Einzelunternehmen*
SCHÖNBERG gegründet 2002

Impressum hier klicken

Ing. Schönberg Christian

Weitere tolle und kostenlose Softwaretools unter:

http://schoenberg.co.at/blog-software

Viren und andere Bedrohungen im Internet

Als **Computervirus** wird ein sich selbst verbreitendes **Computerprogramm** bezeichnet, welches zumeist **schadhafte Veränderungen** am Status der Hardware, am Betriebssystem oder an weiterer Software vornimmt.

1.) Welche Bedrohungen gibt es:

- **Viren, Würmer, Trojaner:** die negativen Auswirkungen reichen von unsinnigen Textmeldungen bis hin zum Löschen sämtlicher Dateien auf dem Computer. Diese können durch Emails oder durch Downloads übertragen werden. Ein Wurm ist ähnlich wie ein Virus, nur dass dieser kein Programm benötigt, an das er sich anhängt. Trojaner sind scheinbar nützliche Programme, in denen sich allerdings ein gefährlicher Virus versteckt.
- **Spyware und Adware:** SpyWare wird sehr oft von Trojanern in den Computer eingeschleust. Diese haben die Aufgabe, das Surfverhalten zu beobachten. Häufig speichern diese aber auch wichtige Daten, wie Kreditkartennummern, usw., indem diese die Tastatureingaben abfangen. Adware hat den Hauptzweck, ungewollte Werbung einzublenden.
- **Browser-Hijacking:** hierbei wird der Benutzer beim Start des Browsers auf eine andere Seite umgeleitet, indem die verantwortlichen Programme die Interneteinstellungen manipulieren.
- **Hoaxes:** sind eine Art Kettenbriefe, bei denen die Empfänger um Geld gebeten werden, usw.
- **Pishing Mails:** diese Mails versuchen, an die Logins und Passwörter der Opfer heranzukommen. Oft sollte der Empfänger auf Seiten geführt werden, die den tatsächlichen Webseiten (z.B. Online-Banking-Zugang) täuschend ähnlich sind.
- **Typosquatting:** dieser Begriff kommt von 'falsch Tippen'. Die Betrüger verwenden Domains, die den von seriösen und bekannten Webseiten sehr ähnlich sind.
- **Spam/Junk-Mail:** Spam kennt fast jeder. Es sind Massenmails, die bereits beinahe alle Internetuser ungewollt erhalten.
- **Kurz-URLs:** diese Kurz-URLs sind zwar sehr beliebt, es wird aber von Betrügern gerne ausgenützt, dass die Zieladresse nicht erkennbar ist. So landet man schnell ungewollt auf einer virenverseuchten Webseite.

Zählpixel

Hacker, Cracker und Skript-Kiddies

Schützen WIE?

Ing. Schönberg Christian

Weitere tolle und kostenlose Softwaretools unter:

http://schoenberg.co.at/blog-software

Kostenloses Softwaretool zum Erstellen sichere Passwörter.

Hier klicken

- **Zählpixel:** diese werden auch Verfolger-Wanze genannt. Dahinter verbirgt sich ein zumeist 1x1 Pixel großes Bild. Dieses wird vom Server von Hackern geladen und die Hacker können dann Daten vom Benutzer sammeln.
- **Flash-Dateien:** Flash Dateien werden sehr häufig verwendet, können aber auch von Hackern missbraucht werden. Vor allem wenn eine Meldung erscheint, dass ein Script installiert werden soll, sollte man vorsichtig sein.
- **Cookies und Super-Cookies:** Cookies sorgen normalerweise dafür, dass Daten auf dem PC gespeichert werden und diese beim nächsten Webseitenbesuch automatisch erkannt werden. Diese Cookies verbergen sich aber auch in vielen Werbebannern und die Betreiber können damit das Nutzerverhalten auslesen.
- **ActiveX-Steuerung:** Diese wurde von Microsoft entwickelt und ist eine Erweiterung für den Internet-Explorer. Vorsichtig sollte man sein, wenn die Quelle unbekannt ist.
- **JavaScript:** diese betreffen alle Browser. JavaScript wird oft zum unbemerkten Umleiten auf Pishing-Seiten verwendet.
- **Hacker, Cracker, Skript-Kiddies:** Wichtig sind vor allem die Beweggründe von Hackern und Crackern. Hacker haben häufig nicht die Absicht einen Schaden anzurichten. Sie möchten vor allem Sicherheitslücken aufdecken. Anders ist dies bei Crackern. Diese handeln nach kriminellen Gesichtspunkten. Besonders gefährlich sind die Skript-Kiddies. Diese sind meistens männliche Jugendliche oder junge Erwachsene deren einziges Ziel es ist, möglichst großen Schaden anzurichten.
- **Internet Abzocke:** Diese Seiten haben das Hauptziel den Opfern das Geld aus der Tasche zu ziehen. Dabei lassen sich diese die unterschiedlichsten Methoden einfallen.

2.) Wie kann man sich schützen:

- **Virenscanner:** diese gehören zum absoluten Muss für jeden Internetbenutzer. Wichtig ist natürlich, dass die Virenschutzsoftware immer am aktuellen Stand ist. Nur so kann ein umfangreicher Schutz bestmöglich gewährleistet werden.
- **Firewall:** die Firewall ist eine Art Wächter zwischen Computer und Internet. Die Firewall kann allerdings keine Viren finden, die sich bereits auf dem Computer befinden.
- **Automatische Windowsupdates:** hierbei ist wichtig, dass diese auf dem Computer eingerichtet bzw. aktiviert ist. Diese normalerweise als Standard eingestellt, sollte nicht geändert werden.
- **Spyware-Schutzprogramme:** Im Rahmen der Windowsupdates wird auch ein Tool zur Entfernung bösartiger Software geladen, das im Hintergrund agiert. Zusätzlich gibt es den Windows Defender. Diese beiden Tools sollten aber nur als Ergänzung verwendet werden.

Weitere tolle und kostenlose Sicherheitstools unter:

Hier klicken

Internetbrowser

Emails

Sichere Kennwörter

Ing. Schönberg Christian

Weitere tolle und kostenlose Softwaretools unter:

http://schoenberg.co.at/blog-software

Datenverschlüsselungstool gratis
Hier_klicken

- **Internetbrowser:** Hierbei sollte versucht werden, immer eine möglichst aktuelle Version installiert zu haben. Zum Beispiel der Internet-Explorer 7 gilt in diesem Hinblick als hoffnungslos veraltet. Außerdem ist es zu empfehlen unter den Einstellungen einzutragen, dass der Browserverlauf bei jedem Beenden des IE gelöscht wird. Dann sollte man es auch in Betracht ziehen, die ActiveX zu deaktivieren. Bei der Cookie-Behandlung sollte mindestens die Stufe Mittel gewählt werden. Verständlicherweise sollte auch der Popup-Blocker aktiviert sein.
- **Emails:** bei Emailsoftware gibt es häufig eine Vorschau oder ein Vorschaufenster. Hierbei ist kritisch, dass bei der Vorschau schon ein Teil des evtl. Schadcodes geladen wird. Daher sollte auf Vorschau verzichtet werden. Zum Standard gehört mittlerweile natürlich der Spamfilter. Ohne diesen würde man womöglich unter den unzähligen Spammails ersticken.
- **WLAN:** Dies ist besonders in dicht gebauten Siedlungen bzw. Wohnungen evtl. kritisch. Wichtig ist hierbei eine WEP- oder WPA-Verschlüsselung, wobei natürlich die WPA-Verschlüsselung zu bevorzugen ist.
- **sichere Kennwörter:** Grundsätzlich ist zu sagen, dass gute Kennwörter vor Gelegenheitseinbrechern schützen, aber einem gezielten Angriff nur zeitlich begrenzt standhalten. Trotzdem ist es wichtig, dass Ihre Kennwörter sicher sind. Hierbei gibt es auch Softwaretools, mit denen sichere Kennwörter erstellt werden können. Beim Browser ist es außerdem zu empfehlen, die Auto Vervollständigung zu deaktivieren.

3.) Zusatzmassnahmen:

- **Ordnerfreigabe im Netzwerk:** Hierbei sollte Kennwort-geschütztes Freigeben verwendet werden.
- **Datenverschlüsselung:** diese ist natürlich zu empfehlen, ist aber bei den meisten Windows-Betriebssystemen erst mit höheren Versionen verfügbar.
- **Daten endgültig löschen:** dies ist vor allem dann wichtig, wenn Sie eine Festplatte oder ein sonstiges Speichermedium wegwerfen möchten. Hierbei sollten Sie alle Daten löschen. Nur in den Papierkorb verschieben ist natürlich zu wenig.
- **Anonym surfen:** Dafür gibt es Secure Proxy Server. Diese sind aber häufig nicht sehr komfortabel. Eine bewährte aber nicht kostenlose Lösung wäre der Notraxx-Stick.
- **Bezahlen im Internet:** Als risikoloseste Methode gilt die Zahlung mit Rechnung und Zahlschein. Auch der Bankeinzug ist aufgrund der 42-tägigen (muss individuell geprüft werden) Widerrufsrecht relativ sicher. Bei Kreditkarten gibt es allerdings schon gewisse Bedenken. Dann gibt es noch die PaySafeCard. Damit ist eine anonyme Bezahlung möglich. Außerdem gibt es noch elektronische Bezahlmöglichkeiten. Diese sollten aber vor der Benützung individuell geprüft werden.
- **HTTPS:** wichtig ist hierbei, dass vor der https:// Adresse sich auch ein symbolisches Vorhangschloss befindet. Außerdem können Sie hierbei auch das Zertifikat prüfen.

FAZIT: Diesbezüglich sind die Einhaltung und konsequente Nutzung von Sicherheitsvorkehrungen, sowie die ständige Achtsamkeit sehr wichtig!