

Viren und Spyware – das sollten Sie beachten!

- genauere Infos zur Durchführung der beschriebenen Schritte im Handbuch -

Computerviren und andere schädliche Programme wie etwa Spyware (Software, die versucht, persönliche Informationen zu erlangen) oder Dialer (Einwahlprogramme, die hohe Telefonkosten verursachen können) stellen heute die wahrscheinlich größte Bedrohung für die Funktionsfähigkeit von PCs dar. Der Service-PC hat bereits zahlreiche Sicherheitsfunktionen, um Sie vor derartigen Programmen zu schützen.

Doch das beste Schloss nützt nichts, wenn Sie dem Einbrecher selbst die Tür öffnen – beachten Sie daher bitte folgende Sicherheitshinweise:

Halten Sie Ihren Computer aktuell

Aktualisieren Sie regelmäßig folgende Programme
AVG AntiVirus (Updates erfolgen größtenteils automatisch)
Spybot Search & Destroy
Firefox (sofern verwendet)
Thunderbird (sofern verwendet)

Auch in Windows werden immer wieder Sicherheitslücken entdeckt. Werden diese nicht umgehend geschlossen, ist Ihr Computer ein leichtes Ziel für Viren.

Updates für Windows werden automatisch aus dem Internet geladen und beim herunterfahren des PCs installiert. In einigen Fällen, z.B. wenn die Zeit, die Sie im Internet verbringen, dafür nicht ausreicht, müssen die Updates von Hand heruntergeladen werden. Sicherheitshalber sollten Sie daher regelmäßig die Seite windowsupdate.microsoft.com besuchen, und alle empfohlenen Updates herunterladen und installieren.

Suchen Sie regelmäßig nach Viren und Spyware

Suche sie alle 14 Tage mit AVG AntiVirus und Spybot nach Viren bzw. Spyware.

Seien Sie vorsichtig bei E-Mails, insbesondere bei Anlagen

Öffnen Sie Anlagen nur dann, wenn Sie sicher sind, dass Sie der Absender selbst an Sie verschickt hat. Oft werden Absender manipuliert oder ein Freund, der Ihnen schreibt, hat selbst einen Virus und verbreitet ihn ohne es zu wissen. Fragen Sie im Zweifelsfall beim Absender nach.

Oft werden auch E-Mails mit dem Ziel versendet, Ihre Kontonummer, PIN oder TANs zu erfahren (Phishing). E-Mails scheinen dann von der eigenen Bank zu kommen, Sie werden aufgefordert auf einen Link zu klicken und dort Angaben zu machen. Ignorieren Sie solche E-Mails, Ihre Bank wird Sie niemals per E-Mail auffordern, irgendwelche geheimen Daten preiszugeben. Wenn Sie wirklich für möglich halten, dass die E-Mail echt ist, fragen Sie telefonisch bei Ihrer Bank nach.

Besuchen Sie nur Websites, denen Sie vertrauen

Aufgrund von Sicherheitslücken in den Internetbrowsern kann schon das Besuchen einer Website reichen, um einen Virus einzuschleusen. Seien Sie insbesondere vorsichtig bei Seiten, von denen illegale Software (WareZ) verbreitet wird und bei Erotikangeboten.