

Handel mit Computern und Bürosystemen - Wien

Ein Computervirus wurde auf Ihrem PC gefunden

Wie kann ich mich schützen und wie erkenne ich eine Infektion?

Viren sind neben Würmern und Trojanern die gefährlichsten Schadssoftwares.

Sie können private Daten ausspähen, diese unbemerkt an dritte weiterreichen, ganze PC-Netzwerke lahmlegen oder Mailserver stark überlasten, sodass Schäden in Milliardenhöhe entstehen.

Wie erkennen Sie eine Infektion?

Nicht jeder Virus kann identifiziert werden. Jedoch sollten Sie bei gewissen Anzeichen misstrauisch werden. Arbeitet der Computer sehr viel langsamer als gewohnt, kann dies ein Indiz für eine im System befindliche Malware sein. Deutlich bemerkbarer wird ein Virus, wenn Meldungen unerwartet erscheinen, Programme unaufgefordert gestartet oder geschlossen werden, oder wenn das Betriebssystem plötzlich heruntergefahren wird. Insbesondere sollten Sie hellhörig werden, wenn E-Mail-Kontakte angeblich E-Mails von Ihnen erhalten haben, die Sie jedoch wissentlich nie verschickt haben.

Präventivschutz

- Schützen Sie Ihr Benutzerkonto mit einem starken Passwort
- Führen Sie regelmäßig Sicherheitsupdates für Ihr Betriebssystem durch.
- Beziehen Sie Updates zu Programmen, sofern diese nicht über ein automatisches Update verfügen, nur von Herstellerwebsites.
- Installieren Sie ein Antivirenprogramm und halten dieses mit Updates auf dem neusten Stand.
- Führen Sie regelmäßig eine Prüfung auf Viren Ihrer gesamten Daten und Datenträger (USB-Sticks, externe Festplatten, usw.) durch.
- Lassen Sie sich die Datei-Endungen im Windows-Explorer bzw. – Finder anzeigen.
- Installieren Sie eine Firewall, die Ihren Datenverkehr zwischen Computer und einem Netzwerk überwacht.
- Erlauben Sie nur bekannten und seriösen Programmen und Anwendungen den Zugriff auf Ihre Netzwerk- und Internetverbindungen.
- Unerwartete E-Mails mit fragwürdigem Absender, Betreffzeile oder Inhalt, sollten nicht geöffnet werden. Bei angefügten Programmen und Links ist Vorsicht geboten! Im Zweifelsfall kann der sichtbare Link manuell in die Adresszeile des Browsers eingegeben werden.
- Antworten Sie nicht auf Spammails und unerwünschte Werbemails. Der Absender kann so erkennen, dass Ihre Mail-Adresse aktiv ist.
- Auf Phishing-Mails, welche die Übermittlung sensibler (Konto-) Daten fordern, am besten nicht reagieren und in den Papierkorb verschieben.

Akutmaßnahmen

- Bewahren Sie Ruhe und schließen Sie alle geöffneten Programme.
- Trennen Sie die Verbindung zum Netzwerk / Internet.
- Überprüfen Sie Ihr gesamtes System mittels des aktuellen Antivirenprogramms.
- Folgen Sie den Empfehlungen des Antivirenprogramms zur Entfernung der Schadssoftware.
- Wiederholen Sie diesen Vorgang ggf. auch mit einem anderen Antivirenprogramm (ACHTUNG: mehrere Antivirenprogramme können sich bei gleichzeitiger Nutzung gegenseitig beeinträchtigen).

Weitere Schritte

- Speichern Sie Ihre ungesicherten Daten auf einem externen Speichermedium.
- Die Schadssoftware kann Änderungen an Ihrem Betriebssystem unternommen haben, installieren Sie Ihr gesamtes System neu, um auf der sicheren Seite zu sein.
- Ändern Sie Ihre Passwörter zu sensiblen Logins.
- So sich mehrere Computer im selben Netzwerk befinden, prüfen Sie auch diese auf Infektion.
- Bereinigen Sie alle Sicherungen, die auch infiziert sein können.
- Löschen Sie die automatischen Wiederherstellungspunkte von Windows um eine Re-Infektion zu verhindern.

Die Gefahr Opfer von Malware zu werden ist trotz der vielen Schutzmaßnahmen immer noch groß und darf deshalb nicht unterschätzt werden. Durch Information sowie aktivem und richtigem Handeln kann das Risiko allerdings gesenkt werden.