Mit Updates den PC sichern

Betriebssysteme, Officeanwendungen, Mediaplayer, Programme die auf das Internet zugreifen und Virenscanner bieten nur dann sicheren Schutz vor Computerschädlingen, wenn sie auf aktuellem Stand sind. Vorhandene Sicherheitslücken und Schwachstellen ermöglichen es Angreifern, Schadprogramme einzuschleusen und die Kontrolle über fremde Systeme zu übernehmen.

Bei manchen Programmen, etwa bei Windows oder den gängigen Virenscannern erleichtern automatische Update-Services die Aktualisierung. Oft ist es aber der Verantwortung der einzelnen Nutzer überlassen, neue Entwicklungen zu verfolgen und die Software durch das Herunterladen und Installieren von Updates vor Viren, Würmern und sonstigen Angriffen zu sichern.

Leider gibt es Programme wie den Flash-Player, der durch eine erzwungene Zustimmung zur Lizenzvereinbarung bei jedem Update und etlichen erforderlichen Klicks für viele Anwender zum Rätsel wird und damit auf vielen System veraltet ist und ein hohes Sicherheitsrisiko ist.

Update-Leitfaden

Man unterscheidet zwischen Funktionsupdates und Sicherheitsupdates.

Funktionsupdates verbessern die Funktion eines Programmes oder fügen neue hinzu. Zum Beispiel werden Programm, dir bisher unter XP liefen, mit Updates WIN7-fähig gemacht oder Grafikprogramme erhalten neue Zeichenfunktionen.

Das Einspielen der Updates ist nicht unbedingt notwendig wenn Sie mit dem Programm zufrieden sind.

Sicherheitsupdates sollten so rasch als möglich eingespielt werden, wenn möglich mit der automatischen Updatefunktion. Sicherheitsupdates sind regelmäßig erforderlich bei Windows (dabei sind alle Bestandteile wie Internetexplorer, Mediaplayer usw. enthalten), Office (auch Open-Office), Virenscanner, Acrobat-Reader, Flash-Player, Shockwave-Player, RealPlayer, Firefox, Chrome usw.

Im Prinzip ist jedes Programm das Dateien von anderen Anwendern öffnen kann gefährdet.

Beachten Sie die folgenden Maßnahmen, damit ihr Computer immer auf dem aktuellen Stand ist.

Verschaffen Sie sich einen Überblick über die wichtigsten von Ihnen eingesetzten Programme!

Dazu zählen neben dem Betriebssystem und dem Browser auch Office-Pakete, Medienplayer, Dienstprogramme von Providern oder das Virenschutzprogramm.

Prüfen Sie, ob bzw. zu welchen Produkten Sie automatische Update-Services erhalten!

Wenn Sie nicht wissen von wem Sie regelmäßig automatisch Updates erhalten, dann sehen Sie in der Online-Hilfe beziehungsweise in den Einstellungen Ihrer Software nach.

Mit Updates den PC sichern

Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken!

Erstellen Sie eine Übersicht darüber, für welche Programme Sie eigenständig auf Updates achten müssen!

Falls Sie feststellen, dass Ihnen für eines oder mehrere zentrale Programme kein automatischer Update-Service zur Verfügung steht, legen Sie sich eine Liste an. Überprüfen Sie dann regelmäßig, ob Updates zur Verfügung stehen.

Informieren Sie sich regelmäßig über Updates – etwa durch Newsletter.

Das Bürger-CERT des BSI bietet ein Newsletter-Service an, der Sie über wesentliche Neuerungen informiert. So sind Sie über aktuelle Updates immer auf dem neuesten Stand. Aber auch einzelne Softwareproduzenten oder Brancheninformationsdienste wie www.heise.de oder www.golem.de stellen Warndienste ("Alert Services") zur Verfügung.

Laden Sie Updates rasch herunter und installieren Sie sie!

Kurz nachdem eine Sicherheitslücke bekannt wird werden Schädlinge verbreitet. Nur so können die Programmierer sie soviel Schaden wie möglich verursachen – oder auch maximalen Profit machen.

ACHTUNG: Lassen Sie sich durch gefälschte Updates nicht aufs Glatteis führen!

Leider wird die Bereitschaft zum Update-Management durch die Programmierer von Computerschädlingen immer wieder für Ihre Zwecke missbraucht: So werden etwa Warn-E-Mails gefälscht und irreführende Popups auf fremde Computer geschmuggelt. Als Richtschnur sollten Sie Updates nur dann installieren, wenn der Hinweis darauf in der Ihnen vertrauten Form erfolgte. Wenn Ihnen E-Mail-Nachrichten mit Aktualisierungshinweisen verdächtig erscheinen, dann folgen Sie den darin enthaltenen Links nicht, sondern informieren Sie sich in Newstickern und tippen Sie die entsprechenden Webadressen manuell ein. Grundsätzlich sollten Sie keine Mailanhänge mit angeblichen Aktualisierungen bzw. Updates öffnen, denn seriöse Firmen verschicken solche Daten nicht per E-Mail.

Achten Sie auf Mitteilungen, die das Auslaufen des Supports für Produkte ankündigen!

Softwareanbieter bieten Aktualisierungen für einzelne Produkte oftmals nur für einen gewissen Zeitraum an. Beispiel dafür ist etwa die Beendigung des Supports für Windows 98 und für Windows XP (mit Service Pack 1) durch Microsoft.

Installieren Sie, wenn erforderlich, Upgrades für neue Programmversionen!

Wenn Hersteller umfassende Änderungen an Ihren Programmen vornehmen, dann erhalten diese Aktualisierungspakete oft eine neue Versionsbezeichnung. Das Programm x in der Version 1.2 wird also beispielsweise durch die Installation eines Upgrades zur Version 1.3. Zumeist sind in solchen Upgrades auch sicherheitsrelevante Änderungen enthalten.