Freie Universität Berlin

{tip4u://093} Version 6

Zentraleinrichtung für Datenverarbeitung (ZEDAT)
www.zedat.fu-berlin.de

Windows 7 - aber sicher

Der Betrieb von PC-Arbeitsplätzen mit Zugang zum Internet bedarf einiger Schutzmaßnahmen. Diese Anleitung beschreibt die Gefahren und Gegenmaßnahmen zum Schutz davor.

zedat

Zentraleinrichtung für Datenverarbeitung
Fabeckstraße 32 / 14195 Berlin
Hotline (030) 838 77777 / hilfe@zedat.fu-berlin.de

Windows 7 - aber sicher

Gefahr aus dem Internet

Rechner mit Zugang zum Internet – sei es über das Campusnetz der FU einschließlich WLAN oder einen anderen Internet-Provider – sind heutzutage leider von Viren, Würmern und anderen Angriffen bedroht. Der Schaden, den solche Angriffe verursachen können, ist vielfältig:

- Rechner stürzen ab und sind unbrauchbar.
- Daten werden gelöscht.
- Vertrauliche Informationen werden ausspioniert (Passwörter, PINs, Kreditkarten-Daten...)

Dieses Verhalten betrifft in der Regel nur den jeweiligen Rechner bzw. dessen Nutzer selbst. In einen Rechner eingedrungene Schadsoftware vermag aber noch mehr. So ist es möglich, einen Rechner ohne Wissen des Besitzers auf verschiedene Weise zu missbrauchen. Beispiele sind:

- die vollständige „Fernsteuerung“ eines Systems
- der Versand von Spam- und Viren-Mails
- das Ablauschen von Daten in lokalen Netzen
- das weltweite Anbieten urheberrechtlich geschützten Materials
- das Aufspüren weiterer potentieller Infektionsopfer und deren Kompromittierung
- Angriffe auf Rechner und Netzwerkkomponenten mit dem Ziel, deren Funktionsfähigkeit zu beeinträchtigen (Denial of Service, DoS)

Es gibt also viele zwingende Gründe, den eigenen Rechner nach besten Kräften so zu schützen, dass Viren, Würmer und deren Verwandte keine Chance haben.

Das Eindringen von Schadsoftware in einen Rechner kann auf verschiedenen Wegen erfolgen. E-Mails und Webseiten können gefährlichen Code enthalten, aber auch ohne Zutun des Nutzers kann Schadsoftware über das Netz in einen Rechner eindringen, weil reguläre aber fehlerhaft oder unzulänglich programmierte Software dies zulässt bzw. nicht verhindert.

Schutzmaßnahmen

Grundsätzlich sollten Sie beim Aufruf fremder Texte bzw. Programme im Web sowie von Links oder Anhängen (Attachments) in Ihren Mails ein gesundes Misstrauen walten lassen: Wollen Sie wirklich das fremde Java-Programm starten, von dem Sie eigentlich gar nicht genau wissen, was es tut? Sind Sie sicher, dass die Ihnen zugesandte Datei, die „man unbedingt gesehen haben“ muss, von einer vertrauenswürdigen Person stammt? ...

Achten Sie bitte ferner darauf, dass Sie nicht als Administrator im Netz „surfen“ oder Mails abrufen, sondern richten Sie sich dafür ein Konto mit eingeschränkten Rechten ein. Dies verringert die Wahrscheinlichkeit, dass systemkritische Funktionen durch Schadprogramme gestört werden.

Eine Reihe vorbeugender technischer Maßnahmen unterstützt darüber hinaus beim Schutz des eigenen Rechners:

Updates für Betriebssystem und andere Programme
: sollten schnellstmöglich installiert werden, um angreifbare Lücken weitgehend auszuschließen.

Anti-Viren-Software
: hilft, bereits das Eindringen von Viren und Ähnlichem zu unterbinden. Die regelmäßige online-Aktualisierung der Virendatenbank ist dabei unerlässlich.

Firewall-Software
: sorgt (korrekt eingesetzt) dafür, dass unerwünschte Netzverbindungen bereits am „Eingang" des Rechners blockiert werden, so dass schädliche Software weniger Chancen zum Eindringen hat.

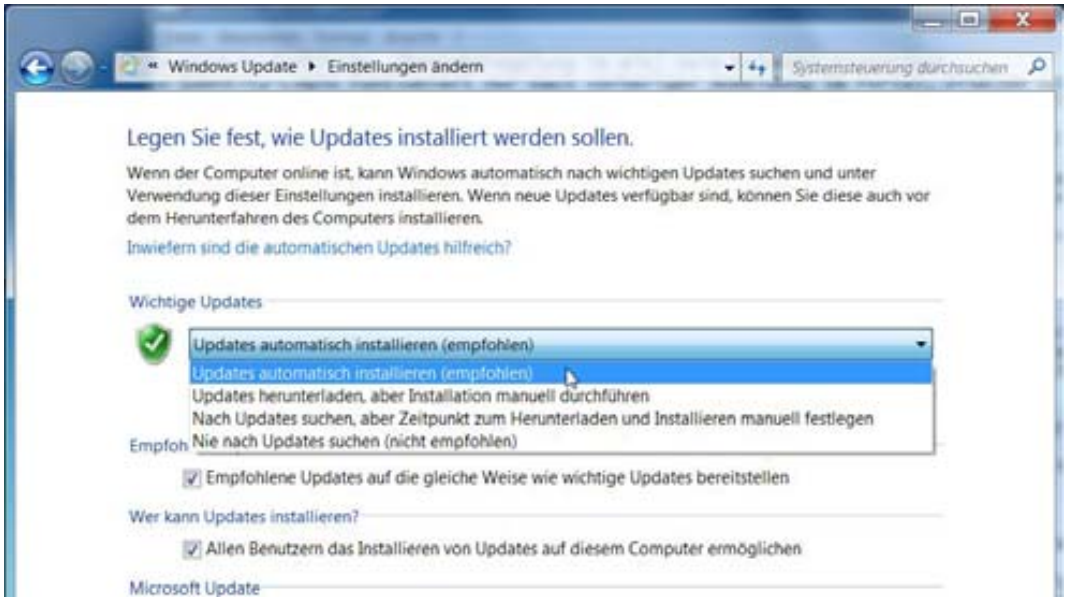
Welche Sicherungsmaßnahmen für einen PC mit Windows 7 erforderlich sind, wird im Folgenden kurz umrissen. Die Erläuterungen gelten im Wesentlichen für Nutzer, die ihren Rechner selbst administrieren. Zentral verwaltete Arbeitsplätze erfordern u.U. andere Verfahren.

Updates für Betriebssystem und andere Programme

Updates automatisch installieren lassen

Windows Updates können über die Systemsteuerung heruntergeladen und installiert werden.

- Benutzen Sie ein Konto mit Administrator-Rechten
- Starten Sie die Systemsteuerung
- Wählen Sie in der Kategorie *System und Sicherheit* den Punkt *Automatische Updates aktivieren oder deaktivieren*
- Im Fenster *Einstellungen ändern* sollte unter *Wichtige Updates* der Punkt *Updates automatisch installieren (empfohlen)* ausgewählt sein. Sollte dies nicht der Fall sein, so klicken Sie mit der linken Maustaste auf die Dropdown-Schaltfläche und wählen den oben genannten Punkt aus. Bestätigen Sie die Einstellung mit *OK*.



- Wählen Sie in der Kategorie *System und Sicherheit* den Punkt *Nach Updates suchen* Klicken Sie auf die Schaltfläche *Nach Updates suchen* und warten Sie, bis die Aktualisierung abgeschlossen ist. Wurden neue Updates gefunden, so klicken Sie auf *Updates installieren*. Da einige der Updates einen Neustart erfordern, müssen Sie eventuell die bisherigen Schritte wiederholen. Erst wenn Sie die Meldung erhalten, dass keine wichtigen Updates (mehr) vorliegen, ist Ihr PC auf dem aktuellen Stand.

- Unter dem vorhergehenden Punkt *Automatische Updates aktivieren oder deaktivieren* können Sie auch automatische Updates für einen beliebigen Zeitpunkt planen.
- Denken Sie aber bitte daran, dass Ihr Computer zur geplanten Zeit eingeschaltet sein muss, damit Updates installiert werden. Sie sollten daher eine Uhrzeit auswählen, zu der Ihr Computer Zugriff auf das Internet hat und nicht etwa für andere wichtige Aufgaben im Netzwerk benötigt wird.

Anti-Viren-Software

Anti-Viren-Software schützt Ihren Computer vor Viren. Auf vielen Computern ist beim Kauf bereits ein derartiges Programm installiert. Falls dies nicht der Fall war, können Sie Anti-Viren-Software jedoch auch selbst installieren.

Egal, ob vor- oder selbst installiert: Es **reicht nicht**, ein Anti-Viren-Programm einmalig zu installieren. Anti-Viren-Programme sind nur dann wirkungsvoll, wenn man sie auf dem aktuellen Stand der Technik hält. Dazu bedarf es unbedingt der aktuellen Programm-Updates sowie der neuesten Virendefinitionen, die man aus dem Netz herunterladen kann. Dieser Updatevorgang kann – ähnlich wie beim Windows-Update – meist so eingerichtet werden, dass er in bestimmten Zeitabständen automatisch erfolgt. Installation und Konfiguration sind natürlich abhängig vom eingesetzten Programm.

Über das Portal der ZEDAT können Sie als Angehöriger der Freien Universität das Anti-Virus-Programm von Sophos kostenlos herunterladen. Eine Anleitung zur Installation finden Sie unter: https://www.zedat.fu-berlin.de/Benutzerservice/Sophos

Firewall

Die Windows-Firewall, die standardmäßig auf Computern mit Windows 7 aktiviert ist, schützt Ihren Computer vor Zugriffen aus dem Internet, indem sie jeden Zugriff von außen nach innen blockt. Netzwerkzugriffe, die eine Verbindung von innen nach außen aufbauen, wie z.B. das Aufrufen einer Webseite oder das Senden und Empfangen von E-Mails, sind davon nicht betroffen.

Dennoch gibt es Programme, die Daten von außerhalb benötigen. Diese Programme erzeugen beim Start eine Windows-Sicherheitswarnung, bei der Sie entscheiden können, ob Zugriffe auf dieses Programm von außen immer geblockt werden sollen, in Zukunft nicht mehr geblockt werden sollen oder ob eine einmalige Blockade erfolgen und beim nächsten Mal erneut gefragt werden soll.

Wenn Sie auf *Zugriff zulassen* klicken, wird eine Ausnahmeregel für dieses Programm definiert. In der Systemsteuerung können Sie unter *System und Sicherheit* die Firewalleinstellung bzw. die Liste der zugelassenen Programme bei *Programm über die Windows-Firewall kommunizieren lassen* anpassen.

Achtung: Das Deaktivieren der Firewall ist ein Sicherheitsrisiko!