



News-Meldung vom 08.03.2010 12:06

## Windows-Tool soll Update-Plagerei überflüssig machen

Alle fünf Tage muss der durchschnittliche Windows-Anwender ein Update installieren oder ein Programm aktualisieren, um eine potenzielle Sicherheitslücke in einer Windows-Anwendung zu schließen. Dabei muss er lernen, mit durchschnittlich 22 unterschiedlichen Update-Mechanismen umzugehen. Zu diesem Ergebnis ist der dänische Sicherheitsdienstleister Secunia in einer **Studie[1]** (PDF) gekommen.

Grundlage der Studie waren die mit dem **Personal Software Inspector[2]** (PSI) anonymisiert gesammelten Daten, etwa welche Software in welcher Version auf dem Rechner installiert ist. PSI untersucht die installierte Software auf bekannte Sicherheitslücken und meldet sie dem Anwender – und Secunia.

90 Prozent der PSI-Anwender mussten demnach in den letzten zwölf Monaten zwischen 51 und 86 mal Hand anlegen, um bis zu 342 Lücken mit Updates zu beseitigen. Dabei konzentrierten sich die Lücken auf Programme von nur 36 Herstellern. Update-Aufwand und -Häufigkeit, um ein System sicher zu halten, überschreite bei weitem das Maß, was ein normaler Anwender gewillt sei, aufzubringen, fasst Secunia in seiner Studie zusammen.

Abhilfe brächte eine einheitliche Patch-Lösung unter Windows, die Programme verschiedener Hersteller überwachen und selbst aktualisieren kann. Eine derartige Funktion für Windows 7 forderte bereits Mitte 2009 der Kommentar "**Mein Wunschzettel für Windows 7: Updates für Alle[3]**" auf heise Security. Bislang verfügbare Update-Manager stellen zwar eine Übersicht der veralteten Software dar und bieten Download-Links zum manuellen Herunterladen sowie Installieren der aktuellen Version, wünschenswert wäre eine automatische Update-Funktion.

Das will Secunia in die **kommende Version 2.0[4]** des Personal Software Inspector integrieren, mit der Anwender ihr System einfach auf dem Laufenden halten können. Eine ähnliche Funktion hat Secunia bereits im Corporate Software Inspector (CSI), der Unternehmenslösung, integriert und getestet.

Linux-Anwender sind fein raus: So gut wie alle Distributionen bieten automatische Updates aller mitgelieferten Pakete an. Nur wer davon abweicht, muss selbst die Augen offen und nach möglichen Sicherheitsupdates Ausschau halten. Selbst nicht freie Software, etwa Adobe Reader und Adobes Flash Player, mittlerweile die am häufigsten genutzten Einfallstore, lassen sich bei vielen Distributionen über Repositories installieren und aktualisieren.

*Siehe dazu auch:*

- **Secunias Personal Software Inspector in Version 1.5 verfügbar[5]**
- **Secunia PSI gibt Empfehlungen zu sicherem Browsing[6]**

(dab[7])

**URL dieses Artikels:**

<http://www.heise.de/security/meldung/Windows-Tool-soll-Update-Plagerei-ueberfluessig-machen-948570.html>

**Links in diesem Artikel:**

[1] [http://secunia.com/gfx/pdf/Secunia\\_RSA\\_Software\\_Portfolio\\_Security\\_Exposure.pdf](http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf)

[2] [http://secunia.com/vulnerability\\_scanning/personal/](http://secunia.com/vulnerability_scanning/personal/)

[3] <http://www.heise.de/security/artikel/Mein-Wunschzettel-fuer-Windows-7-Updates-fuer-Alle-270132.html>

[4] <http://secunia.com/blog/80/>

[5] <http://www.heise.de/meldung/Secunias-Personal-Software-Inspector-in-Version-1-5-verfuegbar-186646.html>

[6] <http://www.heise.de/meldung/Secunia-PSI-gibt-Empfehlungen-zu-sicherem-Browsing-220287.html>

[7] <mailto:dab@ct.de>