

## Online-Gefahren und Schwachstellen wegputzen

G Data gibt Tipps für den erfolgreichen Frühjahrsputz 3.0

(ddp direct) Die Garage auf Vordermann bringen oder den Keller endlich wieder aufräumen, mit dem Beginn des Frühlings steht bei vielen wieder das traditionelle Großreinemachen an. Ein Frühjahrsputz lohnt sich aber nicht nur in den eigenen vier Wänden, sondern auch auf dem Rechner, Smartphone und Tablet-PC. Im Laufe der Zeit sammeln sich hier einige Daten und veraltete Programme an. Dabei stellen gerade die Software-Oldies ein besonders hohes Risikopotential dar, da sie Cyber-Kriminellen ideale Möglichkeiten für erfolgreiche Angriffe bieten. Anwender sollten daher auf ihrer Festplatte ausmisten, verfügbare Programm-Updates installieren und eine Sicherheitslösung installieren, um sich gegen Online-Gefahren abzusichern. G Data unterstützt Internetnutzer beim erfolgreichen Frühjahrsputz 3.0 und hat Tipps für die erfolgreiche Umsetzung und mehr Sicherheit im Internet zusammengestellt.

Die Gefahren durch veraltete Programme werden oft unterschätzt, dabei nutzen Cyber-Kriminelle diese gezielt für Angriffe aus, um so sensible Daten zu stehlen oder Nutzer auszuspionieren?, erklärt Ralf Benz Müller, Leiter der G Data Security Labs. Anwender sollten ihren Rechner daher regelmäßig entrümpeln und alle verfügbaren Software-Updates installieren. Programme, die vom Hersteller nicht mehr aktualisiert werden, sollten deinstalliert werden.

Nach Ansicht des Experten sollten Nutzer beim Frühjahrsputz auch ihre Smartphones und Tablet-PCs nicht vergessen: Bei den Mobilgeräten lohnt sich ein kritischer Blick auf die installierten Apps und deren Berechtigungen. Viele Anwendungen enthalten kritische Befugnisse, die u.a. den Zugriff auf das Adressbuch oder andere persönliche Daten erlauben. Anwender sollten hier überprüfen, ob sie die App wirklich benötigen und diese im Zweifelsfall lieber löschen?, rät Ralf Benz Müller. Für den Fall eines Diebstahls oder Verlust des Smartphones sollte ebenfalls vorgesorgt werden. Hier empfiehlt der IT-Security-Experte den Einsatz einer Sicherheitslösung mit integriertem Diebstahlschutz, um das Mobilgerät orten oder die gespeicherten Daten aus der Ferne löschen zu können.

### G Data Sicherheitstipps für den erfolgreichen Frühjahrsputz 3.0

#### Auf dem Rechner:

Sicherheitslücken schließen: Das Betriebssystem und die installierte Software sollten durch das Einspielen von Service Packs, Patches und Updates auf dem neuesten Stand sein. Veraltete Programme, für die kein Hersteller-Service mehr existiert, sollten umgehend entfernt und ggf. durch eine neue Version ersetzt werden. Die Festplatte aufräumen: Anwender sollten doppelte, veraltete und nicht mehr benötigte Dateien löschen. Beim Aufspüren von doppelten Daten helfen Gratisprogramme, wie z.B. CloneSpy oder AntiTwin. Diese sind u.a. auf den Heft-CDs von PC-Magazinen zu finden. Dateien sollten mit Hilfe eines digitalen Shredders restlos entfernt werden. Diese Funktion ist oft auch in Sicherheitslösungen integriert. Temporäre Dateien löschen: Nutzer sollten in regelmäßigen Abständen die temporären Dateien löschen, die sich im Ordner Temp? im Windows-Verzeichnis befinden und durch das Surfen im Internet entstehen. Das Entfernen dieser Daten führt zu einem deutlich schnelleren Rechner. Passwörter regelmäßig ändern: Passwörter von Nutzerkonten auf dem PC oder im Internet sollten regelmäßig geändert werden. Dabei sollten Nutzer auf sichere Kennwörter setzen und hierzu eine zufällige Folge von Ziffern, Sonderzeichen und Buchstaben in Groß- und Kleinschreibung wählen. Keine Spuren hinterlassen: Browser-Cookies, der Verlauf und Webformulardateien sollten nach jeder Internetsitzung gelöscht werden, da sie Daten vom Surfverhalten aufzeichnen. Eine Konfiguration für die automatische Entfernung kann in den Browser-Einstellungen vorgenommen werden. Einige Browser bieten auch einen privaten Modus an, in dem die meisten temporären Dateien nach der Browsersitzung gelöscht werden. Keine Passwörter im Browser speichern: Nutzer sollten die Funktion Passwörter speichern? im Browser generell deaktivieren. Passwörter, die schon im Browser gespeichert sind, sollten gelöscht werden. Über die Browser-Einstellungen können alle Webseiten mit gespeicherten Kennwörtern eingesehen und gelöscht werden. Geschützt durch Security Software: Anwender sollten eine umfassende Sicherheitslösung nutzen und diese regelmäßig durch Programm- und Virensignaturupdates aktualisieren. Die Verwendung von Security-Lösungen mit einem integriertem System-Tuning und Registry-Cleaning macht das System außerdem schneller und stabiler. Daten sichern: Ein Backup sichert alle wichtigen Daten für den Fall einer Infizierung oder eines Systemcrashes. Durch ein Systemabbild lässt sich außerdem die ganze Festplatte mit allen installierten Programmen sichern. Umfassende Security-Lösungen enthalten häufig ein entsprechendes Modul.

#### Auf dem Mobilgerät:

Installierte Apps überprüfen: Smartphone- und Tablet-Besitzer sollten einen kritischen Blick auf ihre Apps und deren Berechtigungen werfen, denn Updates führen oft auch zu Änderungen bei den Befugnissen der Applikationen, die von Nutzern oft ungelesen akzeptiert werden. Anwender sollten daher jede einzelne App überprüfen und im Zweifelsfall löschen, wenn sie zu viele Berechtigungen umfasst. Eine Berechtigungskontrolle hilft dabei, einen Überblick zu erhalten. Apps nur aus sicherer Quelle beziehen: Anwender sollten nur Applikationen aus vertrauenswürdigen Marktplätzen installieren, z.B. Google Play bei Android-Geräten und App-Märkte der Hersteller. Mobilgeräte schützen: Auf Smartphones oder Tablets sollte eine mobile Sicherheitslösung installiert sein, die das Gerät effektiv vor Mobil-Schadcode und gefährlichen Apps absichert. Diebstahlschutz für das Smartphone: Anwender sollten für den Fall eines Geräteverlusts oder einer Entwendung vorsorgen und einen Diebstahlschutz installieren. Dieser sollte u.a. die Fernsperrung und Lokalisierung des Gerätes und das Löschen aller darauf gespeicherten Daten ermöglichen. Einen Diebstahlschutz umfasst u.a. G Data MobileSecurity 2.

Shortlink zu dieser Pressemitteilung:

<http://shortpr.com/unwxw>

Permanentlink zu dieser Pressemitteilung:

<http://www.themenportal.de/wirtschaft/online-gefahren-und-schwachstellen-wegputzen-76429>

=== G Data gibt Tipps für den erfolgreichen Frühjahrsputz 3.0 (Bild) ===

Die Garage auf Vordermann bringen oder den Keller endlich wieder aufräumen, mit dem Beginn des Frühlings steht bei vielen wieder das traditionelle Großreinemachen an. Ein Frühjahrsputz lohnt sich aber nicht nur in den eigenen vier Wänden, sondern auch auf dem Rechner, Smartphone und Tablet-PC. Im Laufe der Zeit sammeln sich hier einige Daten und veraltete Programme an. Dabei stellen gerade die Software-Oldies ein besonders hohes Risikopotential dar, da sie Cyber-Kriminellen ideale Möglichkeiten für erfolgreiche Angriffe bieten. Anwender sollten daher auf ihrer Festplatte ausmisten, verfügbare Programm-Updates installieren und eine Sicherheitslösung installieren, um sich gegen Online-Gefahren abzusichern. G Data unterstützt Internetnutzer beim erfolgreichen Frühjahrsputz 3.0 und hat Tipps für die erfolgreiche Umsetzung und mehr Sicherheit im Internet zusammengestellt.

Shortlink:

<http://shortpr.com/xuop1f>

Permanenter Link:

<http://www.themenportal.de/bilder/g-data-gibt-tipps-fuer-den-erfolgreichen-fruehjahrsputz-3-0>

=== Ralf Benzmüller, Forschungsleiter G Data Software AG (Bild) ===

Die Gefahren durch veraltete Programme werden oft unterschätzt, dabei nutzen Cyber-Kriminelle diese gezielt für Angriffe aus, um so sensible Daten zu stehlen oder Nutzer auszuspionieren, erklärt Ralf Benzmüller, Leiter der G Data SecurityLabs. Anwender sollten ihren Rechner daher regelmäßig entrümpeln und alle verfügbaren Software-Updates installieren. Programme, die vom Hersteller nicht mehr aktualisiert werden, sollten deinstalliert werden.

Nach Ansicht des Experten sollten Nutzer beim Frühjahrsputz auch ihre Smartphones und Tablet-PCs nicht vergessen: Bei den Mobilgeräten lohnt sich ein kritischer Blick auf die installierten Apps und deren Berechtigungen. Viele Anwendungen enthalten kritische Befugnisse, die u.a. den Zugriff auf das Adressbuch oder andere persönliche Daten erlauben. Anwender sollten hier überprüfen, ob sie die App wirklich benötigen und diese im Zweifelsfall lieber löschen, rät Ralf Benzmüller. Für den Fall eines Diebstahls oder Verlust des Smartphones sollte ebenfalls vorgesorgt werden. Hier empfiehlt der IT-Security-Experte den Einsatz einer Sicherheitslösung mit integriertem Diebstahlschutz, um das Mobilgerät orten oder die gespeicherten Daten aus der Ferne löschen zu können.

Shortlink:

<http://shortpr.com/ck3aj6>

Permanenter Link:

<http://www.themenportal.de/bilder/ralf-benzmueller-forschungsleiter-g-data-software-ag>

=== Online-Gefahren und Schwachstellen wegputzen (Dokument) ===

Die Garage auf Vordermann bringen oder den Keller endlich wieder aufräumen, mit dem Beginn des Frühlings steht bei vielen wieder das traditionelle Großreinemachen an. Ein Frühjahrsputz lohnt sich aber nicht nur in den eigenen vier Wänden, sondern auch auf dem Rechner, Smartphone und Tablet-PC. Im Laufe der Zeit sammeln sich hier einige Daten und veraltete Programme an. Dabei stellen gerade die Software-Oldies ein besonders hohes Risikopotential dar, da sie Cyber-Kriminellen ideale Möglichkeiten für erfolgreiche Angriffe bieten. Anwender sollten daher auf ihrer Festplatte ausmisten, verfügbare Programm-Updates installieren und eine Sicherheitslösung installieren, um sich gegen Online-Gefahren abzusichern. G Data unterstützt Internetnutzer beim erfolgreichen Frühjahrsputz 3.0 und hat Tipps für die erfolgreiche Umsetzung und mehr Sicherheit im Internet zusammengestellt.

Shortlink:

<http://shortpr.com/ohnbw5>

Permanenter Link:

<http://www.themenportal.de/dokumente/online-gefahren-und-schwachstellen-wegputzen>

## Pressekontakt

G Data Software AG

Frau Kathrin Beckert  
Königsallee b 178  
44799 Bochum

[presse@gdata.de](mailto:presse@gdata.de)

## Firmenkontakt

G Data Software AG

Frau Kathrin Beckert  
Königsallee b 178  
44799 Bochum

[gdata.de](http://gdata.de)  
[presse@gdata.de](mailto:presse@gdata.de)

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm. G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter [www.gdata.de](http://www.gdata.de)

Anlage: Bild



Graphic by G Data 2009

