Ronald Eikenberg

www.sicher.surfen

Security-Checkliste Web-Browser

Browser sind ein häufiges Einfallstor für Schädlinge und müssen angemessen abgesichert werden. Auch in Sachen Datenschutz besteht Handlungsbedarf.

Checkliste

- Plug-ins ausmisten
- Click-to-Play aktivieren
- Passwortspeicher verschlüsseln
- Aktuelle Browser-Version nutzen
- Tracking und Skripte einschränken

Plug-ins ausmisten

Browser-Plug-ins wie Flash oder Java sind ein beliebtes Angriffsziel für Hacker – insbesondere unter Windows. Wenn Sie Plug-ins nicht auf dem aktuellen Stand halten, ist Ihr System wahrscheinlich angreifbar. Es genügt, eine verseuchte Website zu öffnen, um sich zum Beispiel einen fiesen Verschlüsselungstrojaner auf den Rechner zu holen, der Ihre Daten in Geiselhaft nimmt. Bei Angreifern stehen vor allem Flash, Adobe Reader, Java und Silverlight hoch im Kurs. Wer kann, sollte auf diese Plug-ins verzichten – insbesondere bei letzteren beiden ist das inzwischen schmerzfrei möglich, da sie kaum noch zum Einsatz kommen.

Kontrollieren Sie zunächst, welche Plug-ins in Ihren Browsern installiert sind und welche verzichtbar sind. Bei Chrome erreichen Sie die Übersicht über die Adresse „chrome://plugins“, bei Firefox über „about:addons“ und einen Klick auf „Plugins“. Firefox weist dort gleich auf als unsicher bekannte Plug-ins hin. Beim Internet Explorer klicken Sie auf das Zahnrad-Symbol, „Add-Ons verwalten“ und „Anzeigen: Alle Add-Ons“. Wer Safari unter Mac OS X nutzt, findet die entsprechenden Optionen unter „Safari/Einstellungen/Sicherheit/Website-Einstellungen verwalten“. Auf den jeweiligen Einstellungsseiten kann man nicht mehr benötigte Plug-ins auch deaktivieren. Deinstalliert werden Sie wie eigenständige Programme, etwa unter Windows über die Systemsteuerung.

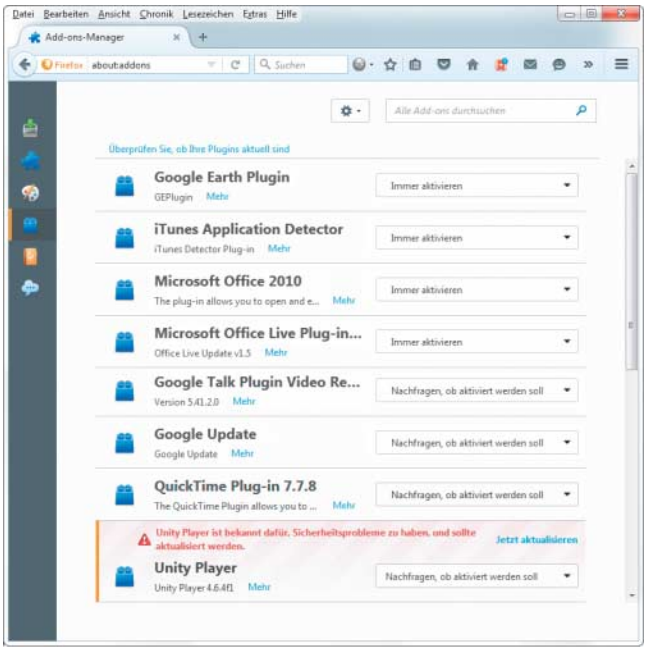
Bringen Sie die übrigen Plug-ins auf den aktuellen Stand. Dafür gibt es keinen einheitlichen Prozess: Einige wichtige Plug-ins bringen einen Updater mit, bei anderen muss man Updates von der Herstellerseite laden und installieren. Besonders leicht haben es die Nutzer von Chrome, da der Google-Browser bereits Flash und einen PDF-Viewer mitbringt und sich um deren Aktualität kümmert. Firefox stellt von Haus aus zumindest PDF-Dateien dar, was die Installation des Adobe Reader erspart. Seit Windows 8 bringt das Betriebssystem einen Flash-Player für die Microsoft-Browser mit und kümmert sich auch um dessen Aktualität. Auch ein einfacher PDF-Viewer ist mit an Bord.

Click-to-Play aktivieren

Die Funktion Click-to-Play stoppt viele Browser-Angriffe effektiv: Ist sie aktiv, werden Plug-ins erst ausgeführt, nachdem Sie zugestimmt haben – etwa durch das Anklicken eines Platzhalters. So kann man zum Beispiel den Flash-Player gezielt für ein eingebettetes Video freischalten, während ein versteckter Flash-Exploit auf der gleichen Seite nicht zur Ausführung kommt. Click-to-Play ist nicht nur sicherer, sondern spart auch noch Ressourcen. Unter Chrome aktivieren Sie Funktion über den Menüknopf und „Einstellungen/Erweiterte Einstellungen/Datenschutz/Inhaltseinstellungen/Plug-in/Selbst auswählen, wann Plug-in-Inhalte ausgeführt werden sollen“. Bei Firefox ändern Sie im Add-ons-Manager „about:addons“ rechts die Einstellung „Immer aktivieren“ auf „Nachfragen, ob aktiviert werden soll“.

Internet-Explorer-Nutzer rufen den Dialog „Add-Ons verwalten“ wie oben beschrieben auf, klicken im Kontextmenü eines Plug-ins auf „Weitere Informationen“ und als Nächstes auf „Alle Sites entfernen“. Safari-Nutzer klicken im Dialog „Website-Einstellungen verwalten“ (siehe „Plug-ins ausmisten“) auf den Namen eines Plug-ins und ändern die Option „Beim Besuch anderer Websites" auf „Fragen“. Im rechten Bereich des Fensters kann man die Einstellung für einzelne Sites tätigen. Beim IE und Safari bezieht sich diese Option auf alle Instanzen eines Plug-ins auf einer Site. Wollen Sie einzelne Plug-in-Elemente aktivieren, können Sie unter Safari zu der Erweiterung ClickToPlugin (siehe c’t-Link) greifen.

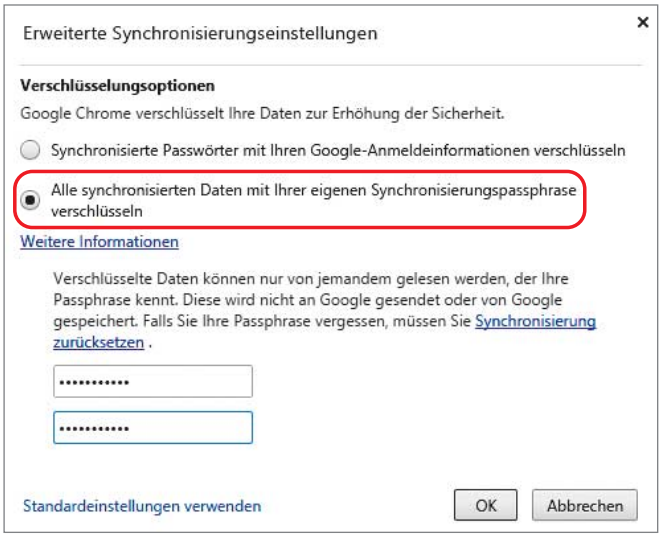
Auch die installierten Browser-Erweiterungen sollten Sie kritisch unter die Lupe nehmen. Erweiterungen haben tiefreichenden Zugriff auf alles, was Sie innerhalb des Browsers tun und können so etwa das Surfverhalten oder Passwörter ausspähen. Sortieren Sie also alles aus, was Sie nicht benötigen. Wer den Edge-Browser von Windows 10 nutzt, muss nicht tätig werden: Der Browser unterstützt mit Ausnahme von Flash weder Erweiterungen noch Plug-ins. Ist ein Browser mit Werbe-Toolbars verseucht, können Sie diese in vielen Fällen mit dem kostenlosen Windows-Tool Avast Browser Cleanup (siehe c’t-Link) loswerden.



Über die Firefox-Einstellungsseite „about:addons“ mistet man verwundbare Plug-ins aus und aktiviert für andere Click-to-Play.

Passwortspeicher verschlüsseln

Wenn Sie den Passwortspeicher von Firefox nutzen, sollten Sie den Zugriff mit einem Master-Kennwort schützen. Es sorgt dafür, dass der Browser Ihre Zugangsdaten verschlüsselt speichert und den Zugriff darauf



Wer die Cloud-Synchronisation von Chrome nutzt, sollte seine Daten mit einem separaten Kennwort schützen – sonst kennt Google sämtliche im Browser gespeicherten Login-Daten.

erst nach Eingabe des Master-Kennworts freigibt. Sie erreichen diese Schutzfunktion zum Beispiel über die URL „about:preferences#security“. Aber Achtung: Wenn Sie das Passwort vergessen, gibt es keine Möglichkeit, die Zugangsdaten im verschlüsselten Passworttresor zu retten.

Unter anderem Firefox und Chrome synchronisieren ihre Zugangsdaten auf Wunsch geräteübergreifend über die Cloud. Bei der Umsetzung werden deutliche Unterschiede in den Unternehmensphilosophien der Hersteller deutlich: Während Firefox die Zugangsdaten vor der Übertragung lokal so verschlüsselt, dass sie für Mozilla nicht einsehbar sind, kann Google sie standardmäßig im Klartext einsehen. Wer das nicht glaubt, kann sich auf der Seite passwords.google.com selbst davon überzeugen. Chrome verschlüsselt die Passwörter lediglich mit Ihrem Google-Passwort – und das kennt Google selbstverständlich. Um zu verhindern, dass Google sämtliche Zugangsdaten erfährt, sollte man sie mit einem separaten Passwort verschlüsseln. Sie finden die Option auf der Einstellungsseite „chrome://settings/syncSetup“ unter „Verschlüsselungsoptionen“.

Aktuelle Browser-Version nutzen

Stellen Sie sicher, dass Sie mit der aktuellen Browserversion surfen, da ein Angreifer Ihren Rechner sonst potenziell über Schwachstellen infizieren kann. Zwar aktualisieren sich Browser wie Chrome und Firefox inzwischen selbstständig, dies gelingt jedoch nicht immer.

Der „Über…“-Dialog zeigt, ob die genutzte Version auf dem letzten Stand ist oder ob es Probleme beim Update-Check gibt. Sie finden ihn bei Chrome nach einem Klick auf den Menüknopf oben rechts unter „Hilfe und Info/Über Google Chrome“ und bei Firefox unter „Menü-Button/Fragezeichen/Über Firefox“.

Sollte das Auto-Update von Firefox inaktiv sein, können Sie es über den Menüknopf und „Einstellungen/Erweitert/Update“ einschalten. Da Chrome und Firefox im laufenden Betrieb keine Updates installieren, ist es wichtig, die Browser immer mal wieder zu beenden. Microsoft aktualisiert Internet Explorer und Edge über Windows Update (siehe S. 74). Um die Aktualität von Safari unter Mac OS X kümmert sich der App Store – auf Wunsch auch automatisch (siehe S. 76).

Tracking und Skripte einschränken

Werbedienstleister, soziale Netzwerke und Tracking-Firmen schauen Ihnen beim Surfen über mehrere Sites hinweg über die Schulter. Um das zu verhindern, können Sie zu einem Tracking-Schutz wie Ghostery (alle wichtigen Browser) oder Privacy Badger (Chrome und Firefox) greifen. Letzterer aktualisiert seine Sperrliste automatisch: Sobald es einen Dienst dabei ertappt, dass er Sie über mehrere Sites hinweg mit eindeutigen IDs trackt, wird er automatisch blockiert. Firefox bietet seit Version 42 einen effektiven Tracking-Schutz, der allerdings nur im privaten Modus aktiv ist. Um ihn dauerhaft für alle Tabs einzuschalten, können Sie in den Experten-Einstellungen „about:config“ den Wert „privacy.trackingprotection.enabled” auf „true“ setzen.

Werbedienstleister wie Googe AdSense werden immer wieder zur Verbreitung von Schadcode missbraucht. Wer auf Nummer sicher gehen und Anzeigen blockieren möchte, kann einen Adblocker wie zum Beispiel uBlock Origin (Chrome, Firefox, Safari) einsetzen. Die Kehrseite der Medaille ist, dass Sie den Betreibern der aufgerufenen Websites eine wichtige Einnahmequelle abschneiden.

Installieren Sie die Erweiterung HTTPS Everywhere (siehe c’t-Link), die dafür sorgt, dass Sie immer auf der verschlüsselt übertragenen HTTPS-Version einer Website landen, wenn es sie gibt. Diese Erweiterung gibt es für Chrome und Firefox. Weitere Tipps zum verschlüsselten Surfen liefert der Artikel „Aber sicher!“ in c’t 25/15, den wir auch kostenlos zum Download anbieten (siehe c’t-Link). (rei@ct.de)

c't Gratis-Artikel und Tools: ct.de/yxwe