Gefahrenquelle Internet

von Thorsten Küfer & Stephan Övermöhle

Die Vernetzung von immer mehr Geräten im Internet erleichtert nicht nur den Informationsaustausch bei der privaten und dienstlichen Nutzung, sie erleichtert auch die missbräuchliche Nutzung. Alle Programme, die mit dem Internet kommunizieren, können missbraucht werden, um persönliche Daten zu sammeln oder um Schadprogramme (engl. Malware) auf dem Rechner zu installieren. Haupteinfallstore für Schadprogramme sind insbes. E-Mails und Webseiten. Zur sicheren Nutzung des Internets sollten deshalb ein paar grundsätzliche Punkte beachtet werden. Im Folgenden werden Sicherheitstipps für das Surfen im Internet vorgestellt.

Sicherheitstipp Nr. 1: Surfen mit Verschlüsselung

Wenn Sie im Internet surfen, sollten Sie darauf achten, möglichst verschlüsselte Webseiten aufzurufen. Ob eine Seite verschlüsselt ist und über ein gültiges Sicherheitszertifikat verfügt, können Sie bei den meisten Browser am Schloss-Symbol sowie am Kürzel „https“ statt „http“ vor der Adresse erkennen (Abb. 1). Dies stellt nicht nur sicher, dass niemand sehen kann welche Inhalte Sie von einer entsprechenden Seite abrufen (Vertraulichkeit), sondern auch, dass Sie nur Inhalte abrufen, die der Seitenbetreiber auch selbst eingestellt hat (Integrität).

Durch zahlreiche Webtechniken (wie z.B. Videos, Flashspiele, Formulare uvm.) haben Sie heutzutage die Möglichkeit, mit den Webinhalten zu interagieren. Leider ermöglichen diese Techniken einem Angreifer bei schlecht gemachten Webseiten, schadhaften Code auszuführen (z.B. mit XSS) und unter Umständen auch mit Ihrem PC zu interagieren. Allein das Aufrufen einer bestimmte Webseite, auf der eine Webtechnik wie Flash- oder JavaScript verwendet wird, kann dazu führen, dass durch Sicherheitslücken im Browser Schadprogramme auf Ihrem PC installiert werden. Unbekannte und zwielichtige Webseiten sollten Sie deshalb möglichst meiden. Das Risiko besteht z.B. wenn Sie über eine Suchmaschine auf neue Webseiten gelangen.

Am einfachsten machen Sie es einem Angreifer aber, wenn Sie seine Schadprogramme selbst herunterladen[1]. Deshalb gilt: Laden Sie Programme nur von Webseiten des Herstellers oder von vertrauenswürdigen Stellen herunter. Am besten sollte die Seite verschlüsselt sein und über ein gültiges Sicherheitszertifikat des Herstellers verfügen. Anhänge in Mails sollten Sie nur dann öffnen, wenn Sie den Absender kennen und auch mit einem Anhang von dieser Person rechnen. Lassen Sie sich ggf. bestätigen, dass die entsprechende Person diese Mail auch wirklich selbst versandt hat. Dies tun Sie am besten per Telefon und nicht per Mail, denn Sie müssen im schlechtesten Fall davon ausgehen, dass der Angreifer die Kontrolle über die Mailadresse Ihres Bekannten hat.

Empfehlung: Da viele Seiten standardmäßig auf ihre unverschlüsselte Variante leiten oder einzelne Teile der Webseite trotzdem unverschlüsselt übertragen, ist es nützlich auch diese Inhalte möglichst automatisiert auf Verschlüsselung umzustellen. Hierzu dient „HTTPS Everywhere“ (https://www.eff.org/HTTPS-everywhere), eine Browser-Erweiterung der Electronic Frontier Foundation (EFF). Sie verschlüsselt Ihre Kommunikation mit Webseiten und erhöht Ihre Sicherheit beim Surfen dadurch signifikant.

Sicherheitstipp Nr. 2: Plug-Ins sparsam Verwenden

Viele Webtechniken benötigen zusätzliche Software damit Sie ausgeführt werden können, sog. Plug-Ins (z. B. Flash oder Java). Es ist empfohlen Plug-Ins nur dann zu installieren, wenn Sie diese auch ganz sicher brauchen. Auch wenn Sie beim Surfen feststellen, dass Sie ein Plug-In benötigen, sollten Sie es nur gezielt freigeben und

[1] Als Negativbeispiel ist hier der Download und die Verwendung einer manipulierten Entwicklungsumgebung von Apple zu nennen, die unter dem Namen XCodeGhost große Wellen geschlagen hat, vgl. z.B. http://heise.de/-2822170.

darauf achten, dass es auf dem aktuellen Stand ist. Besonders das Flash-Plug-In fällt durch Sicherheitslücken regelmäßig negativ auf und sollte daher am besten deinstalliert werden.

Empfehlung: Im Heise Browsercheck (http://www.heise.de/security/dienste/Browsercheck-2107.html) können Sie testen, welche Webtechniken Ihr Browser unterstützt und wie deren Sicherheit eingeschätzt wird. Browser-Erweiterungen (sog. Add-Ons) wie NoScript (https://noscript.net/) (für Firefox), ScriptSafe (für Chrome) (https://www.andryou.com/portfolio/), uMatrix (für Chrome und Firefox) (https://github.com/gorhill/uMatrix/) oder Flashblock (http://flashblock.mozdev.org/) (für Firefox) können Ihnen helfen, Plug-Ins besser zu kontrollieren und bewusster zu nutzen. Dadurch können Sie auf einfache Weise die Sicherheit beim Surfen deutlich erhöhen.

Sicherheitstipp Nr. 3: Filterlisten nutzen

Die meisten Browser nutzen mittlerweile Filterlisten (z.B. Google Safe Browsing), um Webseiten, die erwiesenermaßen böswillig sind und z.B. Schadprogramme verteilen, zu blockieren. Leider ist nach mehreren Fällen in der Vergangenheit nicht mehr auszuschließen, dass Schadprogramme auch über Werbenetzwerke (z.B. Werbebanner) verbreitet werden (vgl.[2] [3]). Die Angreifer kaufen Werbeflächen bei großen Werbe(verteiler)firmen und lassen ihre Inhalte bevorzugt am Wochenende anzeigen. Zu dieser Zeit sind die Firmen meist schwach besetzt, sodass eine Überprüfung der Werbeinhalte nicht oder nur begrenzt stattfindet. Dadurch ist es möglich, dass Sie beim Surfen auf ganz normalen Webseiten mit Schadprogrammen infiziert werden.

Empfehlung: Durch Erweiterungen wie uBlock Origin (https://github.com/gorhill/uBlock) (für Chrome, Firefox und Safari) können Sie über zusätzliche Filterlisten die vom Browser geladenen Inhalte einschränken, dazu gehören z.B. bekannte Adressen für Phishing, Schadprogramme, Tracking und Werbung.

Sicherheitstipp Nr. 4: Tracker und Cookies deaktivieren

Eine weitere Gefahr für Ihre Privatsphäre können Tracker und Cookies sein. Tracker sind Tools, die ihr Surfverhalten analysieren: Sie halten zum Beispiel fest, von wo Sie auf die Seite gelangt sind, wie lange Sie auf der Seite verbleiben und welche Bereiche der Seite Sie sich wie lange ansehen. Auch Cookies sammeln Informationen über Sie und Ihr Verhalten auf einer Webseite. So wird beispielsweise ein Cookie gesetzt, wenn Sie beim Login auf einer Webseite mit einem Häkchen bestätigen, dass Sie „angemeldet bleiben“ möchten. Ab jetzt werden Sie nur noch über den Cookie identifiziert und es wird davon ausgegangen, dass Sie, wenn Sie im Besitz des Cookies sind, auch im Besitz des Passworts sind.

Empfehlung: Cookies stellen ein Sicherheitsrisiko dar und sollten, wenn möglich, in ihrem Browser deaktiviert werden. Möchten Sie auch Tracker blockieren, stehen Ihnen hierfür Erweiterungen wie zum Beispiel Privacy Badger von der EFF (https://www.eff.org/privacybadger) (für Chrome und Firefox) zur Verfügung.

Beachten Sie, dass die oben vorgestellten Erweiterungen zum Teil etwas Einarbeitung benötigen, damit alle Webseiten fehlerfrei dargestellt werden. Eine höhere Sicherheit ist leider immer mit Einschränkungen verbunden. Es sollten nur die tatsächlich verwendeten oder benötigten Erweiterungen installiert werden. Jede zusätzlich installierte Software führt im Zweifel zu einem zusätzlichen Sicherheitsrisiko. Das Ausblenden oder Blockieren von Werbung schadet unter Umständen den Unternehmen, die sich dadurch finanzieren.

Weitere Informationen

Weiterführende Informationen finden Sie auf den Webseiten zur IV-Sicherheit der Uni Münster (https://www.uni-muenster.de/IV-Sicherheit/flyer/), botfrei.de (https://www.botfrei.de/) und bsi-fuer-buerger.de (https://www.bsi-fuer-buerger.de/).

[2] http://heise.de/-921139
[3] http://heise.de/-2400733