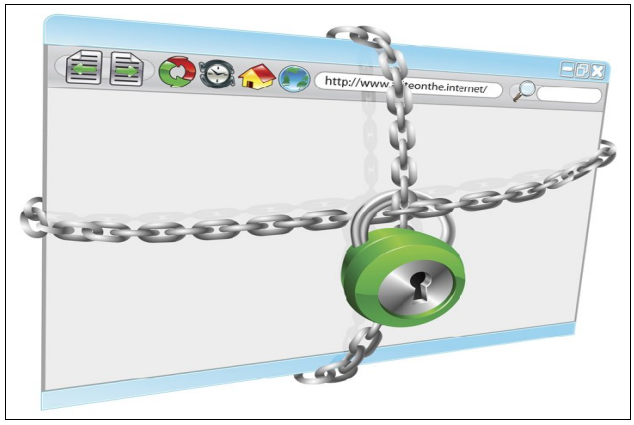
Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitstipp: Browser sicher einsetzen



Der Webbrowser ist für die meisten Internetnutzer das Tor zur Online-Welt. Häufig wird er jedoch auch als Einfallstor für Schadprogramme missbraucht. Kriminelle machen sich unter anderem neu gefundene Sicherheitslecks von sogenannten Browser-Plug-ins zunutze, um Schädlinge einzuschleusen. Das Plug-in *Adobe Flash*, welches das Abspielen von Videos ermöglicht, wies laut dem *BSI-Lagebericht IT-Sicherheit 2011* innerhalb eines Jahres mehr als 50 kritische Sicherheitslücke auf. Diese Zahl ist von besonderer Brisanz, denn Herstellerangaben zufolge ist *Adobe Flash* auf über 99 Prozent aller europäischen PCs installiert [4]. Auch weit verbreitete Plug-ins wie die *Java*-Laufzeitumgebung sind immer wieder Zielscheibe von Angreifern. Ganz entscheidend für die Sicherheit im Internet ist der bewusste Umgang mit dem Webbrowser. Wer Sicherheitsmeldungen aufmerksam verfolgt und gewissenhaft im Internet surft, bleibt öfter von Schadsoftware verschont. In diesem IT-Sicherheitstipp erfahren Sie, wie Sie Ihren Internetbrowser sicher einsetzen.

Vergleichen Sie die Statusleiste Ihres Browsers mit der gewünschten Zieladresse

Der Browser wurde für das Herumstöbern im Netzwerk entwickelt. Dies besagt sein Name, der vom englischen „browse“, zu deutsch „stöbern oder „schmökern“, stammt. Durch das Anklicken von Querverweisen, sogenannten Links, bewegen Sie sich auch auf andere Webseiten. Nicht hinter allen Links verbergen sich vertrauenswürdige Inhalte. Ein Sicherheitsmerkmal stellt hierbei die Statusleiste Ihres Browsers dar. **Bewegen Sie den Mauszeiger auf einen Link und vergleichen Sie ohne zu klicken, ob in der Statusleiste die erwartete Zieladresse erscheint. Ist dies nicht der Fall, so ist es ratsam, dem Link nicht zu folgen, da hierbei im ungünstigsten Falle Schadcode nachgeladen wird.**

Achten Sie bei Online-Diensten auf eine SSL-Verschlüsselung

Einige Online-Dienste wie das Online-Banking erfordern zwingend eine verschlüsselte Kommunikation zwischen Ihrem Browser und dem Server des Dienstleisters. Stellen Sie sicher, dass Sie einen aktuellen Browser verwenden, damit sichergestellt ist, dass dieser gängige SSL-Verschlüsselungen unterstützt. Das SSL-Protokoll gewährleistet Ihnen angemessenen

Schutz, damit Ihre Eingaben von Dritten nicht mitgelesen werden können. Das „https“ in der Adresszeile des Browsers zeigt an, dass der Browser dazu aufgefordert ist, ein SSL-Zertifikat vom Zielserver anzufordern. Nur wenige Zertifizierungsstellen vergeben ein solches Zertifikat an Online-Dienste. Hat Ihr Browser ein geprüftes Zertifikat zurückerhalten, so erfolgen weitere kleine Kommunikationstests zwischen Browser und Server, um auf Nummer sicher zu gehen. Innerhalb kürzester Zeit kann auf diesem Weg eine verschlüsselte Verbindung hergestellt werden. Viele Browser signalisieren das mithilfe eines Vorhängeschlosses in der Statuszeile.

Mittlerweile gibt es einige Erweiterungen für gängige Browsertypen, welche versuchen, ausschließlich verschlüsselte Verbindungen zwischen Server und Browser aufzubauen – so zum Beispiel *KB SSL Enforcer* für *Google Chrome oder Redirect to HTTPS für Opera*. **Ist eine solche Erweiterung installiert, wird schon beim Aufrufen eine Internetseite getestet, ob auch eine sichere Verbindung via SSL möglich ist. Falls der aufgerufene Server also ein gültiges SSL-Zertifikat aufweisen kann, kommunizieren Browser und Server infolge verschlüsselt.** Für *Mozilla Firefox* ist die Erweiterung *HTTPS-Everywhere* empfehlenswert. Sie unterstützt mehr als 1.000 SSL-verschlüsselte Webseiten und sorgt automatisch dafür, dass die betreffenden Webseiten über eine verschlüsselte Verbindung aufgerufen werden.

Weitere Hinweise zur sicheren Kommunikation im Internet finden Sie im IT-Sicherheitstipp *„Sichere Kommunikation über das Internet“* [2]. Beachten Sie für Hinweise zum sicheren Umgang mit dem Internet die Checkliste *„Achte ich auf Sicherheit beim Umgang mit dem Internet?“* [1].

Passen Sie die Browser-Einstellungen Ihren Bedürfnissen an

Viele Internetnutzer verwenden ihren Browser neben dem Austausch sensibler Informationen, wie beispielsweise Log-in-Daten fürs Online-Banking, auch zur Wiedergabe aktiver Inhalte, wie zum Beispiel Videos. Insbesondere aktive Inhalte stellen jedoch ein zusätzliches Sicherheitsrisiko dar, wie der bereits oben genannte Lagebericht des *Bundesamtes für Sicherheit in der Informationstechnik* belegt [4]. Verschärfte Sicherheitseinstellungen in den Optionen Ihres Webbrowsers sind möglich, stellen jedoch einen Komfortverlust beim Surfen dar. Das liegt daran, dass die sogenannten *aktiven Inhalte* einiger Internetseiten bei einem hohen Sicherheitsstandard in ihrer Ausführung eingeschränkt werden. Allen aktiven Inhalten wie beispielsweise *Java* oder *Flash* ist gemein, dass sie nach dem Laden einer aufgerufenen Website im Browser lokal auf dem Rechner des Anwenders ausgeführt werden. Lokal ausgeführte Anwendungen bedeuten stets ein erhöhtes Sicherheitsrisiko, weil sie als Träger von Schadprogrammen aus dem Internet eine direkte Gefahr für Ihr Betriebssystem darstellen können. Aktive Inhalte werden oft für interaktive Anwendungen einer Internetseite, wie beispielsweise Online-Spiele oder auch für das Abspielen von Videos erforderlich. **Sie als Unternehmer sollten sich die Frage stellen, ob Sie nicht zugunsten Ihrer IT-Sicherheit auf den Einsatz der aktiven Inhalte im Webbrowser verzichten können oder diese temporär bei bekannten Gefahren deaktivieren. Stellen Sie in den Browser-Optionen die Sicherheitseinstellungen auf maximal oder deaktivieren Sie ggf. einzelne Plug-ins per Hand.** Hilfreich für die Kontrolle über Plug-ins ist die Erweiterung *(*engl. „Add-on“*) NoScript* für den

Browser *Mozilla Firefox*. Hiermit werden alle unsichtbar ausgeführten Skripte auf Internetseiten sichtbar. Zudem ist es möglich, für verschiedene Internetseiten unterschiedliche Plug-in-Einstellungen vorzunehmen.

Speichern Sie Ihre Passwörter niemals automatisch

Die meisten gängigen Browser geben Nutzern die Möglichkeit, Benutzernamen und Passwörter zu Online-Diensten, wie dem E-Mail-Postfach, automatisch zu speichern. Ist die Option aktiviert, muss der Anwender beim Besuch der betreffenden Website nur das gespeicherte Passwort bestätigen, um sich anzumelden. Diese Browser-Funktion erscheint auf den ersten Blick sehr praktisch, birgt jedoch eine große Gefahr: Sollte sich ein Unbefugter Zugriff zum Benutzerkonto des Anwenders verschaffen, so erhält dieser sämtliche Zugänge zu allen Online-Diensten, deren Zugangsdaten der Browser automatisch gespeichert hat.

Deaktivieren Sie daher die automatische Passwort-Speicherfunktion und das „Auto-Vervollständigen“ in den Optionen Ihres Browsers und nutzen Sie einen Passwort-Manager wie *KeePass X* [3], der Ihre Passwörter sicher verwaltet.

Aktivieren Sie alle Warnmeldungen und Hinweise in den Browser-Einstellungen

Während eines Seitenbesuchs laufen viele Prozesse unbemerkt im Hintergrund ab. **Um mehr Transparenz darüber zu erhalten, welche Daten beispielsweise verschlüsselt oder unverschlüsselt übertragen werden oder wann eine Seite versucht, ein Add-on automatisch zu installieren, sollten Sie in den Optionen Ihres Browsers alle Warnmeldungen und -hinweise aktivieren.** So haben Sie die Gelegenheit, unerwünschte Seitenumleitungen, Downloads oder die Ausführung von unbekannten Scripten zu unterbinden.

Löschen Sie regelmäßig Ihren Browser-Verlauf

Generell ist es ratsam, den Verlauf besuchter Websites in Ihren Browser-Einstellungen regelmäßig zu löschen. Moderne Browser verfügen auch über Einstellmöglichkeiten, die es Ihnen erlauben, generell keine Daten besuchter Webseiten zu speichern. So verhindern Sie, dass nachfolgende Nutzer des PCs oder auch Unbefugte, die sich Zugang zum System verschafft haben, nachvollziehen können, welche Internetseiten Sie besucht haben. Die Benutzung von Online-Diensten an fremden Rechnern stellt ein großes Sicherheitsrisiko dar. Denn Sie können sich nicht sicher sein, ob der PC eventuell mit Spionagesoftware infiziert ist. **Geben Sie daher an öffentlich zugänglichen Rechnern niemals sensible Informationen, wie Passwörter, ein.**

Laden Sie Software nach Möglichkeit nur von Herstellerseiten herunter

Wenn Sie den Browser nicht nur zum Surfen, sondern auch zum Herunterladen von Software verwenden, sollten Sie stets überprüfen, ob die Dateien aus seriöser Quelle stammen. **Laden Sie Software nur direkt von der Seite des Herstellers herunter und nur, wenn Sie sicher sind, dass es sich um einen vertrauenswürdigen Anbieter handelt. Bedenken Sie, dass Sie neben dem bewussten Downloaden von Software auch unbewusst Dateien aus dem Internet herunterladen.** Dies gilt beispielsweise für PDF-Dokumente, die Sie direkt von einer Webseite öffnen. PDFs werden in der Regel nicht wie ein Webseiten-Link direkt aufgerufen, sondern zuerst heruntergeladen und in den temporären Dateien abgelegt. Auch vor dem Öffnen eines Dokumentes sollten Sie sich also stets darüber im Klaren sein, aus welcher Quelle das jeweilige PDF-Dokument stammt.

Seien Sie immer up to date

Veraltete Browser-Versionen sind nicht selten Ursache dafür, dass Schadcode aus dem Internet mittels sogenannter *Drive-By-Exploits* [4] auf den Rechner des Anwenders gelangt. Hierbei werden Sicherheitslücken im Browser oder in den Browser-Plug-ins gezielt ausgenutzt, sobald der Nutzer eine Webseite aufruft, die mit Schadcode infiziert ist. Es besteht demnach die Gefahr, sich schon beim „Vorbeisurfen“ einen Virus oder Trojaner einzufangen, ohne überhaupt irgendetwas auf der Webseite angeklickt zu haben. Drive-By-Exploits finden nicht nur auf den Internetseiten dubioser Dienstleister statt, sondern auch unbeabsichtigt von Webseitenbetreibern: Kriminelle spähen nicht selten Zugangsdaten von schlecht gesicherten Webservern aus und schleusen so Schadsoftware auf die sonst seriösen Webseiten des Betreibers.

Damit Sie sich vor der unsichtbaren Gefahr der Drive-By-Exploits schützen können, sollten Sie regelmäßig und unmittelbar nach dem Erscheinen Software-Updates für Ihren Internetbrowser, Ihre Browser-Plug-ins und Ihr Betriebssystem einspielen. Vergewissern Sie sich beispielsweise mithilfe der automatischen Update-Funktion, dass Sie stets mit der neuesten Version surfen. Das *Institut für Internet-Sicherheit* hat den kostenlosen Dienst *securityNews* entwickelt, der Sie über aktuelle Gefahren im Internet und neue Sicherheitsupdates zahlreicher Programme und Browser-Plug-ins kurz nach dem Erscheinen informiert [2].

Autoren

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen

[1] http://www.kmu-sicherheit.de

http://www.ec-net.de

[2] https://ratgeber.it-sicherheit.de

[3] http://www.sicher-im-internet.de

[4] https://www.bsi.bund.de

https://www.internet-sicherheit.de

http://www.bsi-fuer-buerger.de

http://www.sicher-im-netz.de

Bildquelle: © Christos Georghiou - Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de