Thema: Browsersicherheit Datum: 26.9.2022
Fach: Software Name: Finn Rosendahl
Fachlehrer: Herr Hengesbach Klasse: ITA11

Warum ist Browsersicherheit wichtig?

Da Browser sehr viel verwendet werden stellen sie einen guten Angriffspunkt dar. Angreifer können Fehler und Features im Browser verwenden um Schadsoftware auf dem Computer des Opfers zu installieren oder im schlimmsten Fall komplette Kontrolle über das Gerät erhalten. Über das Internet wird auch sehr viel Schadsoftware verbreitet und manchmal kann man sich nicht sicher sein wem man vertrauen kann. In solchen Fällen ist es gut wenn der Browser vor Schadsoftware warnt oder diese direkt blockiert. Online kommt es auch sehr viel dazu dass persönliche Informationen wie Passwörter, Name, Adresse und ähnliches gestohlen werden. Viele Unternehmen versuchen so viel wie möglich über Nutzer herauszufinden um diese identifizieren zu können und verkaufen diese Informationen dann an andere weiter.

Welche Risiken gibt es?

Sicherheitsrisiken werden größtenteils durch Plug-ins, Erweiterungen, Javascript und Cookies dargestellt. Plug-ins und Erweiterungen sollen dem Browser mehr Funktionalität geben, können leider aber auch für schädliche Zwecke verwendet werden, da sie vollen Zugriff über den Browser, die in ihm gespeicherten Daten und Website-Aktivitäten des Nutzers erlangen können. JavaScript wird verwendet um einer Website mehr Funktionen zu geben, kann aber verwendet werden um zwischen mehreren verschiedenen Seiten Skripte auszuführen und so persönliche Daten stehlen. Webseiten können alle möglichen Daten in Cookies speichern. Manche tun es damit man sich nicht jedes mal neu anmelden muss, manche nutzen es für andere Zwecke. Cookies können allerdings auch verwendet werden, um genaueres über einen Nutzer herauszufinden. Webseiten können die gespeicherten Cookies sehen und so genau herausfinden welche Seiten der Nutzer besucht und somit was seine Interessen sind, Wenn jemand zugriff auf einen Cookie erhält, indem Anmeldedaten gespeichert sind, kann dieser auch verwendet werden um sich ohne das Passwort zu wissen anzumelden. In Acht nehmen sollte man sich auch vor Irreführender Gestaltung und Werbung. Jeder hat wahrscheinlich schonmal einen falschen Download-Button gesehen, welcher auf Schädliche Webseiten oder Downloads leiten kann.

Wie kann ich mich schützen?

Man sollte einen sicheren Browser verwenden und die richtigen Browsereinstellungen treffen (dazu später mehr). Browser Features wie JavaScript sollten nur aktiviert sein, wenn sie absolut nötig sind. Nicht unbedingt benötigte Erweiterungen sollten deaktiviert werden. Ein Contentblocker ist sehr empfohlen. Es gibt noch viele andere nützliche Erweiterungen die die Sicherheit verbessern können (dazu später mehr). Man sollte immer so wenig Cookies wie möglich behalten und auch auf keinen Fall Passwörter im Browser speichern. Man sollte immer Aufpassen wo man hinklickt, vorallem auf nicht sehr seriösen Seiten, weil es sehr einfach sein kann sich einen Virus herunterzuladen. Außerdem ist es eine gute Idee mehrere Email-Adressen für verschiedene Zwecke zu haben, um nicht alle Accounts auf eine Person zurückzuleiten. Es kann auch nützlich sein verschiedene Browserprofile für verschiedene Zwecke zu haben, um bestimmte Daten nicht miteinander zu verbinden.

Browserempfehlungen

Firefox: Ein sehr privater und sicherer Browser, der viele Erweiterungen bietet um die Sicherheit noch mehr zu erhöhen. Er benötigt allerdings viel manuelles Einstellen.
Librewolf: Ein auf Firefox basierender Browser, der ein paar nützliche Features hinzufügt und schon vorkonfiguriert ist.
Brave: Dieser Browser ist auch sehr darauf ausgelegt privat und sicher zu sein. Er hat sehr nützliche Optionen, hat Tor integriert und basiert auf Chromium.
Tor: Der privateste und sicherste Browser, blockiert sehr viele schädliche Objekte und Skripte, kann aber etwas langsamer sein weil er Anfragen durch mehrere Server leitet.

Einstellungen

Die Einstellungen der Browser Firefox, Librewolf, Brave und Chrome wurden getestet. Alle Browser hatten die Optionen Cookies zu blockieren oder automatisch zu löschen, Pop-ups zu blockieren, einen Nur HTTPS Modus zu aktivieren, DNS über HTTPS zu leiten und Berechtigungen wie Standort, Kamera, Mikrofon und Benachrichtigungen zu verwalten.

Die Browser bieten allerdings auch teilweise Einstellungen, die bei anderen nicht vorzufinden waren.
Firefox kann Tracking-Elemente blockieren, Fingerprinting reduzieren und gefährliche und betrügerische Inhalte blockieren.
Librewolf bietet die selben Funktionen wie Firefox, fügt aber das blockieren von Seitenübergreifender Verfolgung, erweiterten Schutz gegen Fingerprinting und das Blockieren von Websiteverbindungen wenn kein SSL-Zertifikat vorliegt hinzu.
Brave bietet einen eingebauten Werbeblocker, kann Tracking-Elemente blockieren, Javascript deaktivieren und Fingerprinting reduzieren.
Chrome bietet lediglich die Optionen JavaScript zu deaktivieren und eine Do-Not-Track Anfrage zu senden, was sehr viel schlechter ist als Tracking-Elemente zu blockieren da Webseiten sich auch einfach entscheiden können diese zu ignorieren.

Suchmaschinen

DuckDuckGo: Speichert keine persönlichen Daten wie IP oder Suchanfragen, beeinflusst die Suchergebnisse nicht, hat eine Browsererweiterung und einen Browser für Handys mit nützlichen Funktionen, hat(te) allerdings einen Deal mit Microsoft ihre Tracker nicht zu blockieren.
SearX: Speichert auch keine persönlichen Daten, bietet erweiterte Sicherheitsoptionen wie z.B. Bilder durch einen Proxy-Server zu leiten um die IP-Adresse zu schützen. Es ist keine eigene Suchmaschine sondern eine Meta-Suchmaschine, das bedeutet es benutzt viele andere Suchmaschinen um nach ergebnissen zu suchen, diese kann man selbst auswählen für verschiedene Kategorien wie Allgemeines, Bilder, Videos, Dateien, Wissenschaft, IT und Social Media. An die Suchmaschinen werden natürlich keine persönlichen Daten gesendet. SearX ist außerdem Open-Source und selbst Hostbar, sodass man sich wirklich sicher sein kann dass niemand die Suchanfragen sieht.

Browsererweiterungen

uBlock Origin: Ein Content-Blocker, kann Werbung, JavaScript, externe Schriftarten und Pop-ups blockieren. Man kann für jede Seite individuelle Regeln festlegen, falls man irgendwo bestimmten Content erlauben möchte. Es gibt viele Voreingestellte Filterlisten mit Dingen die blockiert werden sollen, welche man aktivieren oder deaktivieren kann.
ClearURLs: Diese Erweiterung entfernt Tracking-Elemente aus URLs. Wenn man z.B. bei Amazon etwas sucht und dann ein Ergebnis anklickt stehen in der URL sehr viele zusätzliche Daten, die verwendet werden um z.B. die ursprüngliche Suchanfrage und andere Informationen zu speichern. Das macht es erstens einfacher verfolgt zu werden, und zweitens können Leute mit denen man den Link teilt diese Informationen auch sehen.
Universal Bypass/Auto Link Bypasser: Einfache Erweiterungen die Werbe-Links wie z.B. von adf.ly zu überspringen. Universal Bypass ist für Firefox-Browser, Auto Link Bypasser für Chromium.
User Agent Switcher: Der User Agent gibt Webseiten sehr viele Informationen über den Browser und das Betriebssystem, was einen sehr identifizierbar macht. Diese Erweiterung macht es möglich den User Agent zu ändern, um diese Informationen zu verstecken. Man kann auch für einzelne Seiten eigene User Agents festlegen, um Tracking zu erschweren.
CookieAutoDelete: Diese Erweiterung macht es sehr einfach Cookies zu verwalten. Man kann auswählen welche Cookies man behalten möchte, die anderen werden beim Schließen des Browsers gelöscht.
DuckDuckGo Privacy Essentials: Die Browsererweiterung von DuckDuckGo blockiert viele Tracking-Elemente auf Webseiten. Sie bietet außerdem die möglichkeit, zufällige Email-Adressen zu generieren, welche dann an die normale Adresse weiterleiten. So kann man für jeden Account eine eigene Mail-Adresse haben und diese auch individuell deaktivieren falls man über sie keine Mails mehr empfangen möchte oder sie nur als Wegwerf-Adresse brauchte.
Malwarebytes Browser Guard: Eine Browsererweiterung zum Antivirus Malwarebytes. Während meiner Meinung nach ein Antivirus nicht nötig ist und Windows Defender komplett reicht solange man einen gut funktionierenden Verstand hat, ist diese Erweiterung doch recht nützlich. Sie kann schädliche Elemente blockieren und den Nutzer vor Bedrohungen auf Webseiten warnen.