Bayerisches Staatsministerium für
Unterricht und Kultus

Browser

Stand: 15.01.2025

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / browser

Sichere Nutzung von Browsern

Browsersicherheit schafft Datensicherheit ©Robert Avgustin - stock.adobe.com

Empfehlungen zur Nutzung von Browsern

Der Browser ist eine der am häufigsten genutzten Anwendungen auf dem Endgerät. Er ermöglicht den Zugriff auf eine Vielzahl von Internetangeboten, Webanwendungen und Clouddiensten auf Webservern. Unter Berücksichtigung der nachfolgend aufgeführten Aspekte lässt sich die Sicherheit bei der Nutzung dieser Angebote erhöhen:

- Sicherer Aufruf von Webseiten
- Regelmäßiges Löschen zwischengespeicherter, insbesondere personenbezogener, Daten
- Datensparsame Nutzung und sicherheitsrelevante Einstellungen an Browsern bei Endgeräten, die von mehreren Personen genutzt werden

Die nachfolgenden Klapptexte liefern weitere Informationen zur sicheren Nutzung von Browsern.

Sichere Kommunikation

Die Verschlüsselung der Übertragungsdaten zwischen Browser und Webserver ist inzwischen Standard. Moderne Browser zeigen dies durch ein Symbol (z.B. ein Schloss) in der Adressleiste an. Nur wenn der Webserver die Verschlüsselung unterstützt und ein gültiges Zertifikat nachweisen kann, wird der Browser die Verbindung als gesichert markieren.

TLS (Transport Layer Security) ist das aktuelle Verfahren bzw. Protokoll zur sicheren Internetkommunikation. Es wird von allen aktuellen Browsern unterstützt und ist automatisch aktiv, wenn eine Webseite über HTTPS (Hypertext Transfer Protocol Secure) aufgerufen wird. Der Aufruf einer verschlüsselten Verbindung erfolgt durch die Eingabe von "https://" vor der Webadresse in der Adressleiste des Browsers. In vielen Fällen leiten Webserver automatisch von HTTP auf HTTPS um, um eine sichere Verbindung zu gewährleisten.

Hinweis

Die Tatsache alleine, dass die Verbindung verschlüsselt ist und durch ein gültiges Zertifikat verifiziert werden konnte, ist noch keine Garantie dafür, dass die aufgerufene Seite keine bösartigen Inhalte, wie beispielsweise Malware oder Phishing-Formulare, bereitstellt.

Umgang mit Downloads

Beim Arbeiten im Internet lädt der Nutzende Dateien (z. B. Bilder, pdf-Dateien usw.) herunter, die standardmäßig im Download-Verzeichnis des Betriebssystems gespeichert werden. Auf diese Weise können sich so schnell viele Dateien ansammeln, die beträchtlichen Speicherplatz belegen können. In diesen Dateien können auch **personenbezogene Daten** (z. B. Anhänge von E-Mails, Klassenlisten etc.) enthalten sein, die regelmäßig gelöscht werden sollten.

Das regelmäßige Löschen des Inhalts des Download-Ordners führt nicht nur zu mehr freiem Speicherplatz, sondern schützt auch vor ungerechtfertigter Vorhaltung personenbezogener Daten.

Umgang mit Browsercache und Cookies

Bei jedem Zugriff auf einen Webserver werden Daten übertragen. Eine Speicherung dieser Daten durch den Browser reduziert die zu übertragende Datenmenge, beispielsweise bei erneutem Aufrufen von Bildern. Die lokale Verfügbarkeit der Inhalte fördert den schnellen Aufbau der Webseite, da die Daten bereits im Zwischenspeicher (Cache) des Endgerätes abgelegt wurden.

Der Zugriff auf diese Inhalte ermöglicht jedoch umfangreiche Rückschlüsse auf das

Surfverhalten. In Abhängigkeit vom jeweiligen Nutzungsprofil des Nutzers sowie des genutzten Endgerätes ist eine regelmäßige Löschung des Caches zu empfehlen.

Die regelmäßige Löschung des Caches gewährleistet, dass keine personenbezogenen Daten auf dem Endgerät zurückbleiben und der verfügbare Speicherplatz freigegeben wird. Der zuvor beschriebene Prozess kann zudem über die Browsereinstellungen automatisiert werden, sodass nach Beendigung der Browsernutzung alle zwischengespeicherten Daten gelöscht werden.

Neben den Inhalten einer Webseite werden im Browser ergänzende Informationen gespeichert, sogenannte "Cookies". Diese Informationen dienen unterschiedlichsten Zwecken, wie beispielsweise der Erfassung des Besuchs einer Webseite oder der Steigerung der Nutzerfreundlichkeit. Cookies können sowohl technisch notwendige Funktionen erfüllen als auch Komfortfunktionen in der Nutzung von Browsern bereitstellen. Dazu zählt beispielsweise die Unterstützung beim Ausfüllen von Formularen oder beim Speichern von Online-Warenkörben.

Über Cookies lässt sich aber auch das Surfverhalten der Nutzenden, deren Wege über verschiedene Webseiten oder deren Klickverhalten analysieren.

Zur Sicherung der Privatsphäre besteht die Möglichkeit, Cookies regelmäßig oder automatisch beim Schließen des Browsers zu löschen. Die Konfiguration erfolgt über das Menü „Einstellungen“ des Browsers. Sie ist über das Stichwort „Cookies“ in der Suchfunktion der Einstellungen zu finden.

Umgang mit Passwörtern

Bei einer Anmeldung auf einer Webseite ist die Eingabe persönlicher Zugangsdaten erforderlich. Browser bieten die Möglichkeit, die erforderlichen Daten zu speichern, welche im Passwortspeicher des Browsers hinterlegt werden.

Sofern eine andere Person Zugriff auf das Endgerät und damit auf die Browserdaten hat, besteht die Möglichkeit, sich mit vorgetäuschter Authentizität bei den gespeicherten Webseiten anzumelden. Dies birgt ein beträchtliches Sicherheitsrisiko.

Daher ist es unerlässlich, den Zugriff auf das Endgerät sowie die gespeicherten Zugangsdaten durch ein komplexes Passwort zu schützen.

Es ist nicht immer gleich nachvollziehbar, ob Passwörter lokal auf dem Endgerät oder in einem Cloud-Konto des Browserherstellers gespeichert werden. Eine Speicherung in einem Cloud-Konto sollte wohlüberlegt sein, da dem Anbieter vertraut werden muss.

Besser ist es, dass auf eine Speicherung im Browser verzichtet wird und stattdessen ein Passwort-Manager zum Einsatz kommt. Oftmals bieten Passwort-Manager auch die Möglichkeit der Generierung von sicheren und komplexen Passwörtern.

Zugriff auf Gerätefunktionen

Webseiten und deren integrierte Anwendungen können Zugriff auf bestimmte Gerätefunktionen (z. B. Kamera, Mikrofon oder Standort) verlangen. Als Beispiel sei hier das Videokonferenztool ViKo der ByCS angeführt, welche ohne die Einbindung von Kamera und Mikrofon nicht sinnvoll nutzbar ist.

Der Zugriff auf den Standort ist auf die unbedingt erforderlichen Funktionen bei mobilen Endgeräten zu beschränken. Es sollte grundsätzlich überprüft werden, ob der Standort tatsächlich für die ordnungsgemäße Funktion erforderlich ist.

Im Zweifelsfall sollten Berechtigungen im Nachgang wieder entzogen oder gar nicht erst erteilt werden.

Die erteilten Berechtigungen können über das Menü „Einstellungen“ des Browsers eingesehen werden. Sie sind meist über das Stichwort „Berechtigungen“ in der Suchfunktion der Einstellungen zu finden.

Multi-User und Kiosk-Nutzung

Im Kontext schulischer Nutzung ist es nicht ungewöhnlich, dass ein Gerät von mehreren Personen verwendet wird. In pädagogischen Einrichtungen wie Klassenzimmern, Bibliotheken oder Lehrerzimmern stehen den Schülerinnen und Schülern sowie dem Lehrpersonal Endgeräte zur gemeinsamen freien Nutzung zur Verfügung, wobei mitunter eine benutzerindividuelle Authentifizierung nicht erforderlich ist.

Unter den genannten Einsatzbedingungen ist eine automatische Löschung temporärer Daten (u. a. Cache, Browserverläufe, Cookies) nach jeder Sitzung erforderlich. Dadurch wird auch der unbefugte Zugriff auf personenbezogene Daten verhindert. Gleiches gilt für das Download-Verzeichnis. Die entsprechenden Einstellungen sind ggf. auf administrativer Ebene vorzunehmen.

Es empfiehlt sich die Verwendung des Privat- bzw. Inkognito-Modus (Funktionsbezeichnung ist vom Browser abhängig). Dabei werden beim Schließen des Fensters automatisch benutzerbezogene Informationen, wie der Verlauf und Cookies, gelöscht. Auch offene Websitzungen werden beendet. Zu beachten ist jedoch, dass Dateien, die heruntergeladen wurden, auch in diesem Modus auf dem Endgerät verbleiben und manuell gelöscht werden müssen.

Browsererweiterungen (Plug-Ins)

Browsererweiterungen, sogenannte Plug-Ins, sind kleine Programme, die dem Browser zusätzliche Funktionen hinzufügen. Ihre Funktion besteht in der Erweiterung des Funktionsumfangs, der Erhöhung der Sicherheit oder der Blockierung unerwünschter Werbung.

Die Verwendung von Browsererweiterungen sollte mit Vorsicht erfolgen, da diese potenziell Zugriff auf sensible Daten haben. Es wird empfohlen, Erweiterungen nur aus vertrauenswürdigen Quellen zu installieren und diejenigen zu wählen, die regelmäßig aktualisiert werden. Die Anzahl der installierten Zusatzfunktionen sollte mit Bedacht gewählt werden, da jede Erweiterung ein zusätzliches Sicherheitsrisiko birgt. Die geforderten Berechtigungen der Browsererweiterungen müssen hinsichtlich des Anwendungszwecks kritisch geprüft werden.