Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI für sichere Web-Browser

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 19.09.2019

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[1] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[3] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Analog „Informationssicherheitsbeauftragte (ISB)“
[2] Zur standardisierten Vorgehensweise siehe BSI (2019a)
[3] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Behörde“ verwendet.

Inhaltsverzeichnis

1 Beschreibung

Web-Browser dienen dem Abruf und der Darstellung von Daten aus dem Internet, wie beispielsweise Hypertext, Bildern, Video-, Audio- und anderen Formaten.[4] Die Nutzung von Zusatzfunktionalitäten (z. B. Darstellung bestimmter Medienformate) erfordert häufig die Einbindung von Erweiterungen[5] beziehungsweise die Nutzung externer Bibliotheken des Betriebssystems oder dritter Parteien.

Bei Nutzung eines Web-Browsers werden Daten in der Regel auch aus nicht vertrauenswürdigen Quellen geladen. Diese Daten können schädlichen Code (Viren, Trojaner, Spyware etc.) enthalten und den Arbeitsplatzrechner unbemerkt infizieren, so dass ein sicherer Betrieb nicht mehr möglich ist.[6] Dies kann zum Verlust der Verfügbarkeit, Vertraulichkeit und Integrität schützenswerter Daten führen. Somit stellt eine Nutzung von Web-Browsern grundsätzlich ein Risiko dar. Durch die Umsetzung und Einhaltung dieses Mindeststandards sollen diese Risiken minimiert werden. Er beschreibt Sicherheitsanforderungen an Web-Browser, die auf Arbeitsplatzrechnern der Bundesverwaltung eingesetzt werden. Web-Browser, die auf mobilen Plattformen wie Android oder iOS eingesetzt werden oder ausschließlich auf sichere, interne Netze zugreifen können, sind nicht Gegenstand dieses Mindeststandards.

Bedarfsträgern mit hohem oder sehr hohem Schutzbedarf wird der Einsatz erweiterter Lösungen empfohlen. Dazu gehören insbesondere virtualisierte Systeme[7] oder auch Remote-Controlled-Browser-Umgebungen.[8]

Die in Kapitel 2 beschriebenen Sicherheitsanforderungen beziehen sich auf Konfiguration, Auslieferungszustand und Darstellungskomponenten des Web-Browsers sowie auf Interaktionen mit der Betriebssystemumgebung. Auch wenn Browser nicht traditionell über Ausschreibungen beschafft werden, muss dennoch an einem Punkt eine Entscheidung für ein Produkt getroffen werden. Vor Einsatz eines Web-Browsers ist daher zu prüfen, ob die in Kapitel 2.1 und 2.2 aufgeführten Sicherheitsanforderungen an Browser und Entwicklung vollständig durch den Anbieter implementiert und umgesetzt sind. Dabei haben Anbieter zu belegen (z. B. anhand einer Produktdokumentation), ob und wie ihre Produkte die gestellten Anforderungen erfüllen.[9] Abseits der Beschaffung selbst ist zu überprüfen, ob die Sicherheitsanforderungen an den Betrieb (siehe Kapitel 2.3) erfüllt sind.

Generell gilt, dass ein Web-Browser nicht schon im Auslieferungszustand alle Anforderungen erfüllen muss, er muss es aber ermöglichen, ihnen über organisatorische Maßnahmen oder Erweiterungen von Drittanbietern gerecht zu werden. In zentral verwalteten Umgebungen können auch entsprechend geeignete und dokumentierte zentrale Sicherheits- und Überwachungslösungen bestimmte Sicherheitsanforderungen abdecken.

In Anlehnung an den IT-Grundschutz[10] werden die Anforderungen mit den Modalverben „MUSS“ und „SOLLTE“ sowie den zugehörigen Verneinungen formuliert. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

[4] Vgl. BSI (2019b), APP.1.2 Web-Browser
[5] Unter *Erweiterungen* fallen im Sinne dieses Mindeststandards sämtliche Zusatzkomponenten, wie Add-ons oder Plug-ins, die optional installiert werden können, um die Funktionalität von Web-Browsern zu erweitern.
[6] Vgl. BSI (2018a)
[7] Vgl. BSI (2016), S. 25f
[8] Vgl. BSI (2008)
[9] Eine Abgleichstabelle zwischen den Mindestanforderungen und den für die Bundesverwaltung relevantesten Web-Browsern kann auf https://bsi.bund.de/mindeststandards unter „Sichere Web-Browser“ heruntergeladen werden.
[10] Vgl. BSI (2017), S. 18
[11] Vgl. IETF (1997)
[12] Vgl. DIN (2018)

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung/Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

2 Sicherheitsanforderungen

2.1 Technische Sicherheitsanforderungen an Anbieter und Produkt

SW.2.1.01 – Vertrauenswürdige Kommunikation

a) Der Web-Browser MUSS Transport Layer Security (TLS) gemäß dem Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)[13] unterstützen.

b) Der Web-Browser MUSS folgende Anforderungen an Zertifikate und deren Überprüfung erfüllen:

- Eine Liste von Zertifikaten vertrauenswürdiger Zertifikatsaussteller (Certification Authority; CA-Zertifikate) MUSS bereitgestellt werden.
- Zertifikate mit domainbasierter Validierung (Domain-Validated-Zertrifikate, DV), mit organisationsbasierter Validierung (Organizational-Validated-Zertifikate, OV) sowie Zertifikate mit erweiterter Prüfung (Extended-Validation-Zertifikate) MÜSSEN unterstützt werden.
- Eigene Wurzelzertifikate MÜSSEN ergänzt werden können
- Der schreibende Zugriff auf den Zertifikatsspeicher DARF NUR mit administrativen Rechten oder mit der expliziten Zustimmung des Benutzers erfolgen. Insbesondere muss ein lokaler Widerruf von Zertifikaten möglich sein.
- Der Web-Browser MUSS eine vollständige Überprüfung der Gültigkeit des Serverzertifikats durchführen. Diese Prüfung betrifft neben dem Serverzertifikat alle weiteren CA-Zertifikate der Zertifikatskette bis zum Wurzelzertifikat. Die Überprüfung beinhaltet die mathematische Prüfung des Zertifikats mit Hilfe des öffentlichen Schlüssels des ausgestellten CA-Zertifikats sowie die Prüfung der zeitlichen Gültigkeit des Zertifikats und die Überprüfung des Sperrstatus des Zertifikats (Certification Revocation List (CRL) oder Online Certificate Status Protocol (OCSP)).[14]

c) Der Web-Browser MUSS die Kommunikationsform geeignet und nicht manipulierbar darstellen.[15]

- Dem Benutzer MUSS angezeigt werden, ob die Kommunikation mit dem Web-Server verschlüsselt oder im Klartext erfolgt (beispielsweise durch Symbole, farbliche Hervorhebungen oder Anzeige der Protokolle wie „http“ oder „https“).
- Dem Benutzer MUSS ein fehlendes CA-Zertifikat im Zertifikatsspeicher oder ein ungültiges/widerrufenes Serverzertifikat als Prüfergebnis signalisiert werden. Die verschlüsselte Verbindung DARF dann NICHT ohne explizite Bestätigung durch den Benutzer aufgebaut werden.
- Es MUSS dem Benutzer möglich sein, sich die gesamte Domain inklusive aller Subdomains der aktuellen Webseite anzeigen zu lassen.

d) Der Web-Browser MUSS HTTP Strict Transport Security (HSTS) unterstützen. Die Implementierung SOLLTE RFC 6797[16] entsprechen, abweichende Implementierungen zum Schutz des Nutzers vor Tracking (Trackingschutz) sind jedoch zulässig, sofern sie die gleichen Sicherheitsziele erreichen.

[13] Der Mindeststandard TLS fordert aktuell den Einsatz von TLS mindestens in der Version 1.2 in Kombination mit Perfect Forward Secrecy (PFS). Vgl. BSI (2019c)

[14] Das BSI hat das Certification Path Validation Test Tool (CPT) veröffentlicht, das genutzt werden kann, um die korrekte X.509-Zertifikatspfadvalidierung des Web-Browsers nach RFC 5280 (vgl. IETF 2008) zu überprüfen. Diese Maßnahme ist insbesondere bei erhöhten Sicherheitsanforderungen oder beim Einsatz unbekannterer oder älterer Web-Browser zu empfehlen. Das CPT kann unter https://www.bsi.bund.de/CPT heruntergeladen werden.

[15] Typischerweise findet sich diese Funktion oben links neben dem Adressfeld der Browser, wo Details von TLS-Verbindungen mit Schloss-Symbolen und/oder farblichen Hinweisen visualisiert werden.

[16] Vgl. IETF (2012)

SW.2.1.02 – Updates

a) Es MUSS einen Update-Mechanismus für den Web-Browser geben. Update-Mechanismen MÜSSEN folgende Anforderungen erfüllen:

- Update-Mechanismen MÜSSEN sämtliche Web-Browserkomponenten umfassen (inkl. Erweiterungen). Eigenständige Programme, die zusätzlich Elemente in den Browser einfügen (z. B. EXE-Dateien für Internet Explorer, die Buttons einrichten), MÜSSEN über separate Update-Prozesse aktuell gehalten oder untersagt werden.
- Updates MÜSSEN erkannt werden.
- Updates MÜSSEN zuverlässig angezeigt werden.
- Automatisches Einspielen von Updates MUSS möglich sein.

b) Integritätsprüfungen der Updates MÜSSEN folgende Anforderungen erfüllen:

- Updates DÜRFEN NUR dann eingespielt werden, wenn die Prüfung der Integrität ein positives Prüfergebnis liefert.
- Nicht korrekte Prüfergebnisse MÜSSEN dem Benutzer oder Administrator signalisiert werden.

SW.2.1.03 – Browsereigene Kennwortmanager

Wird ein browsereigener Kennwortmanager genutzt, MÜSSEN folgende Sicherheitsanforderungen erfüllt sein:

- Eine direkte und eindeutige Beziehung zwischen Webseite (URL) und hierfür gespeichertem Kennwort MUSS zuverlässig möglich sein.
- Kennwörter MÜSSEN verschlüsselt abgespeichert werden.
- Es MUSS die Möglichkeit geben, den Zugriff auf gespeicherte Kennwörter durch ein Master-Kennwort zu schützen und bei jeder neuen Browser-Sitzung eine erneute Authentisierung zu erfordern.
- Bereits gespeicherte Kennwörter und das Master-Kennwort MÜSSEN auf Anforderung des Benutzers gelöscht werden können.

SW.2.1.04 – Schutz vertrauenswürdiger Daten

a) Der Web-Browser MUSS folgende Einstellungen für Cookies bereitstellen:

- Das Anlegen von Cookies MUSS auf Anforderung des Benutzers deaktiviert werden können.
- Bereits angelegte Cookies MÜSSEN auf Anforderung des Benutzers und automatisch beim Beenden des Web-Browsers gelöscht werden können.
- Die Nutzung von Drittanbieter-Cookies MUSS auf Anforderung des Benutzers blockiert werden können.

b) Der Web-Browser MUSS folgende Einstellungen für Website-Daten und den Browserverlauf bereitstellen:

- Website-Daten sowie der Browser-Cache MÜSSEN auf Anforderung des Benutzers gelöscht werden können.
- Der Browserverlauf und die Liste der Auto-Vervollständigungen MÜSSEN auf Anforderung des Benutzers gelöscht werden können.
- Funktionalitäten zur Auto-Vervollständigung (Name, Email, usw.) MÜSSEN auf Anforderung des Benutzers deaktiviert werden können.

c) Der Administrator MUSS die Übertragung von Nutzungsdaten konfigurieren und deaktivieren können, um ein Auslesen der Nutzungsdaten durch den Hersteller zu vermeiden.

SW.2.1.05 – Überprüfung auf schädliche Inhalte

Wenn adress- oder inhaltsbasierte Schutzmechanismen implementiert sind, die mit externen Diensten kommunizieren, MÜSSEN diese durch den Administrator deaktiviert werden können.

SW.2.1.06 – Same-Origin-Policy

Die Same-Origin-Policy MUSS umgesetzt sein.[17] Insbesondere DÜRFEN Dokumente und Skripte (Client) NICHT auf Ressourcen (z. B. Grafiken, Textfelder) anderer Webseiten zugreifen. Herkunft (Origin) einer Webseite MUSS als Kombination aus den Parametern „Protokoll“ (Schema), „Host", „Port" und „Domain“ in der Adresse (URL) ausgewertet werden. Ein Zugriff auf Ressourcen DARF NUR erfolgen, wenn alle Parameter in der URL identisch sind.

SW.2.1.07 – Sichere Konfiguration

a) Eine Oberfläche für die Verwaltung der Einstellungen MUSS bereitstehen. Einstellungen, um Erweiterungen und JavaScript aktivieren und deaktivieren zu können, MÜSSEN vorhanden sein.

b) Der Import von zentral erstellten Konfigurationen MUSS möglich sein.

c) Sofern vorhanden, MUSS eine Synchronisation mit externen Speicherdiensten und -orten (sog. Cloud-Dienste) deaktivierbar sein.

d) Wenn Browser-Anwendungen ein unterschiedliches Sicherheitsniveau haben (z. B. interne Fachanwendungen, allgemeine Anwendungen und das Internet), MUSS der Web-Browser parallel in unterschiedlichen Konfigurationen betrieben werden können.[18]

SW.2.1.08 – Minimale Rechte

Der Web-Browser MUSS nach seiner Initialisierung mit minimalen Rechten im Betriebssystem ablaufen. Die Managementkomponente (Ressourcenmanager) DARF NICHT dauerhaft die Rechte eines Administrators erfordern, um ablaufen zu können. Bei der Initialisierung DARF der Web-Browser mit erweiterten Rechten laufen, diese MUSS er aber danach wieder abtreten. Lese- und Schreibzugriffe der Darstellungskomponenten DÜRFEN NUR auf festgelegte Bereiche des Dateisystems zulässig sein. Aufrufe von Betriebssystemfunktionen durch Darstellungskomponenten DÜRFEN NUR über wohldefinierte Schnittstellen der Ressourcenmanager erfolgen.

SW.2.1.09 – Sandboxing und Kapselung

a) Der Web-Browser MUSS eine Architektur mit folgenden Eigenschaften bereitstellen:

- Sämtliche Komponenten MÜSSEN voneinander und zum Betriebssystem hin gekapselt sein.
- Direkter Zugriff auf Ressourcen isolierter Komponenten DARF NICHT möglich sein.
- Kommunikation zwischen den isolierten Komponenten DARF NUR über definierte Schnittstellen erfolgen.
- Darstellungskomponenten für aktive Inhalte wie Flash und JavaScript MÜSSEN vom Hauptprozess gekapselt sein.

b) Webseiten MÜSSEN voneinander isoliert werden. Die Isolierung SOLLTE in Form eigenständiger Prozesse erfolgen. Eine Isolation auf Thread-Ebene ist aber auch zulässig.

SW.2.1.10 Content Security Policy (CSP)

Der Web-Browser MUSS die Content Security Policy mindestens in Level 2.0 (CSP 2.0) gemäß den W3C-Spezifikationen[19] umsetzen.

SW.2.1.11 Subresource Integrity

Der Web-Browser MUSS Subresource Integrity (SRI)[20] gemäß den W3C-Spezifikationen umsetzen.

[17] Vgl. Mozilla (2019)
[18] Alternativ kann dies auch auf anderem Wege abgedeckt werden, bspw. über einen zweiten Browser (vgl. BSI 2018b).
[19] Vgl. W3C (2016a)
[20] Vgl. W3C (2016b)

2.2 Organisatorische Sicherheitsanforderungen an Anbieter und Produkt

Die folgenden organisatorischen Sicherheitsanforderungen haben Anbieter im Rahmen von Entwicklung und Wartung des Web-Browsers zu gewährleisten.

SW.2.2.01 – Entwicklung

Es DÜRFEN NUR Programmiersprachen und -werkzeuge verwendet werden, die sichere Funktionen unterstützen und Mechanismen zum Stack- und Heapschutz implementieren. Der Web-Browser MUSS die vom Betriebssystem bereitgestellten Speicherschutzmechanismen nutzen können.

SW.2.2.02 – Aktualisierung

Der Hersteller MUSS Sicherheitsupdates für den Web-Browser bereitstellen. Bei kritischen Schwachstellen[21] SOLLTE der Hersteller innerhalb von 21 Tagen, nachdem ihm die Schwachstelle bekannt wurde, ein Update bereitstellen.

SW.2.2.03 – Kontaktmöglichkeit

Um potenzielle Schwachstellen melden zu können, MÜSSEN Kontaktmöglichkeiten zu Sicherheitsteams des Anbieters bereitgestellt werden.

SW.2.2.04 – Transparenz

Funktionen des Web-Browsers, die auf dem IT-System gespeicherte Daten verändern oder Daten exfiltrieren können, MÜSSEN transparent dokumentiert sein, damit die Auswirkungen auf die Sicherheit bewertet werden können.

2.3 Sicherheitsanforderungen an den Betrieb

Die Wirksamkeit von Sicherheitsmechanismen ist neben den bereits aufgeführten Sicherheitsanforderungen ebenso im Kontext des Betriebs eines Web-Browsers zu betrachten. Daher haben Betreiber die im Folgenden aufgeführten Sicherheitsanforderungen umzusetzen.

SW.2.3.01 – Betriebssystem

Das Betriebssystem des Arbeitsplatzrechners MUSS dem Web-Browser Speicherschutzmechanismen bereitstellen, wie z. B. Address Space Layout Randomization (ASLR), No-execute (NX) bit beziehungsweise Data Execution Prevention (DEP) oder eine sichere Ausnahmebehandlung zum Filtern von Systemaufrufen.

SW.2.3.02 – Administration

a) Es MUSS ein Prozess zur Pflege von Zertifikaten vorgehalten werden (siehe SW.2.1.01b).

b) Es MUSS ein Prozess für die unverzügliche Produktaktualisierung vorgehalten werden (siehe SW.2.1.02).

c) Es MUSS ein Prozess für die Verwaltung der Konfiguration vorgehalten werden (siehe SW.2.1.07).

SW.2.3.03 – Erweiterungen

Die Installation von Erweiterungen auf Arbeitsplatz-PCs MUSS durch Vorgaben geregelt sein und SOLLTE zentral verwaltet werden. Dem Benutzer SOLLTE NUR die Installation von Erweiterungen einer zentralen Whitelist erlaubt werden.

SW.2.3.04 – Basiskonfiguration

Die Behörde MUSS den Web-Browser in folgender Basiskonfiguration ausliefern:

a) Das Protokoll TLS MUSS gemäß dem Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)[22] aktiviert sein.

[21] Eine Schwachstelle wird als kritisch bezeichnet, wenn sie nach dem Industriestandard *Common Vulnerability Scoring System (CVSS) v3.1* mit *High* (7.0 - 8.9) oder *Critical* (9.0 - 10.0) bewertet wird (vgl. FIRST 2019).

[22] Vgl. BSI (2019c)

b) Es MUSS geprüft werden, ob die Liste der Root-CAs eingeschränkt werden muss.

c) Die Nutzung von HSTS MUSS für alle Webseiten aktiviert sein. Abweichungen bei Vorliegen besonderer Geheim- und Datenschutzanforderungen sind möglich.[23]

d) Cookies von Drittanbietern DÜRFEN NICHT akzeptiert werden.

e) Die Ausführung von Erweiterungen zur Medien-Wiedergabe DARF NUR nach Bestätigung des Benutzers erfolgen (Click-to-Play).

f) Encrypted Media Extensions (EME)[24] MÜSSEN deaktiviert werden, wenn diese nicht benötigt werden.

g) Die Funktion zur Auto-Vervollständigung MUSS deaktiviert sein.

h) Das Speichern von Kennwörtern in browsereigenen Kennwortmanagern SOLLTE deaktiviert sein.

i) Das Vorab-Laden von Seiten SOLLTE deaktiviert sein.

j) Die Abfrage gespeicherter Zahlungsmethoden MUSS deaktiviert sein.

k) Flash MUSS deaktiviert sein.

l) Die integrierten Darstellungsmechanismen des Web-Browsers MÜSSEN aktiviert sein und bevorzugt verwendet werden.

m) Adress- oder inhaltsbasierte Schutzmechanismen, die mit externen Diensten kommunizieren, SOLLTEN deaktiviert sein.

n) Die Synchronisation von Daten (Cookies, Chronik, Lesezeichen, etc.) mit externen Speicherdiensten beziehungsweise -orten (Cloud) MUSS deaktiviert sein.

o) Zentral vorgegebene Konfigurationen MÜSSEN vor Änderungen durch den Benutzer geschützt werden können.

p) Wenn Browser-Updates eingespielt werden, MUSS überprüft werden, ob diese die Konfiguration verändern.

SW.2.3.05 – Überprüfung auf schädliche Inhalte

Es MÜSSEN Schutzmechanismen wie z.B. Content-Filter eingesetzt werden, die den Aufruf als schädlich eingestufter Webseiten verhindern.[25]

SW.2.3.06 – Kennwortmanager

Browsereigene Kennwortmanager erfüllen in der Regel nicht die Anforderungen einer Behörde an die Informationssicherheit. Es SOLLTEN daher externe Kennwortmanager genutzt werden. Bei Nutzung eines Kennwortmanagers MUSS das Masterkennwort den verbindlichen Vorgaben der Behörde entsprechen.[26]

SW.2.3.07 – Updates/Patches

a) Der Betreiber MUSS Updates nach SW.2.2.02 dieses Dokuments unverzüglich einspielen.

[23] Da HSTS zum Tracken der Nutzer missbraucht werden kann, muss hier eine Abwägung zwischen Sicherheit und Datenschutz getroffen werden. Daher sollte gemeinsam mit den Informationssicherheits-, Geheim- und Datenschutzbeauftragten entschieden werden, ob ein ggf. möglicher Tracking-Datenabfluss toleriert werden kann. Soll aus Datenschutzgründen auf den Einsatz von HSTS verzichtet werden, muss das entstehende Sicherheitsrisiko bewertet und getragen werden. Diese Entscheidung ist zu dokumentieren.

[24] Vgl. W3C (2016c)

[25] Das BSI betreibt ein zentrales Schadsoftware-Präventions-System (SPS) für den IVBB, das auch für die Netze des Bundes (NdB) fortgeführt wird. Es fungiert als kontinuierlich gepflegte Blacklist, so dass die Anforderung für angeschlossene Behörden grundsätzlich erfüllt ist. Dennoch sollte geprüft werden, ob zusätzliche, individuelle Maßnahmen notwendig sind.

[26] Vgl. BSI (2019b), ORP.4.A8 Regelung des Passwortgebrauchs

b) Unabhängig von der Verfügbarkeit eines Updates MUSS der Betreiber spätestens 7 Tage nach Bekanntwerden einer kritischen Schwachstelle[27] Maßnahmen zur Mitigation ergreifen. Dies KANN bspw. im Rahmen der vom BSI empfohlenen 2-Browser-Strategie die zwischenzeitliche Abschaltung des betroffenen Browsers bedeuten.

c) Falls für den verwendeten Web-Browser keine Sicherheitsupdates mehr zur Verfügung gestellt werden, MUSS gemäß UP Bund[28] schnellstmöglich eine Umstellung auf einen neuen Web-Browser erfolgen. Dies MUSS regelmäßig (mindestens jährlich) geprüft werden.

[27] Eine Schwachstelle wird als kritisch bezeichnet, wenn sie nach dem Industriestandard Common Vulnerability Scoring System (CVSS) v3.1 mit High (7.0 - 8.9) oder Critical (9.0 - 10.0) bewertet wird (vgl. FIRST 2019).
[28] Vgl. BMI (2017), Kapitel 7.2.

Literaturverzeichnis

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund – Leitlinie für Informationssicherheit in der Bundesverwaltung, 2017

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS), BSI-PP-0040, Version 1.0, 2008

BSI (2016) Bundesamt für Sicherheit in der Informationstechnik: Sichere Inter-Netzwerk Architektur SINA, BSI-BRO16/322

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2018a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Empfehlung für sichere Web-Browser, BSI-CS 071, Version 2.0 vom 11.07.2018

BSI (2018b) Bundesamt für Sicherheit in der Informationstechnik: Absicherungsmöglichkeiten beim Einsatz von Web-Browsern, BSI-CS 047, Version 2.0 vom 11.07.2018

BSI (2019a) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758, abgerufen am 12.04.2019

BSI (2019b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 2. Edition 2019

BSI (2019c) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 zur Verwendung von Transport Layer Security, Version 2.0 vom 05.04.2019

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

FIRST (2019) Common Vulnerability Scoring System (CVSS), Version 3.1

Mozilla (2019) Mozilla: Same-origin policy, https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy, abgerufen am 12.04.2019

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119 abgerufen am 25.07.2019

IETF (2008) Internet Engineering Task Force: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, https://tools.ietf.org/html/rfc5280 abgerufen am 22.03.2019

IETF (2012) Internet Engineering Task Force: HTTP Strict Transport Security (HSTS), RFC 6797, I2012, https://tools.ietf.org/html/rfc6797 abgerufen am 20.06.2018

W3C (2016a) World Wide Web Consortium: Content Security Policy 2.0, 2016, https://www.w3.org/TR/CSP2/, abgerufen am 12.04.2019

W3C (2016b) World Wide Web Consortium: Subresource Integrity, 2016, https://www.w3.org/TR/SRI/, abgerufen am 12.04.2019

W3C (2016c) World Wide Web Consortium: Encrypted Media Extensions, 2016, https://www.w3.org/TR/2016/WD-encrypted-media-20160610/, abgerufen am 12.04.2019

Abkürzungsverzeichnis

ASLR	Address Space Layout Randomization
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CPT	Certification Path Validation Test Tool
CRL	Certificate Revocation List
CSP	Content Security Policy
DEP	Data Execution Prevention
EME	Encrypted Media Extensions
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
IT	Informationstechnik
IVBB	Informationsverbund Berlin-Bonn
NdB	Netze des Bundes
NX	No-execute
OCSP	Online Certificate Status Protocol
PFS	Perfect Forward Secrecy
RFC	Request for Comments
SINA	Sichere Inter-Netzwerk-Architektur
SPS	Schadsoftware-Präventions-System
SRI	Subresource Integrity
TLS	Transport Layer Security
URL	Uniform Resource Locator
W3C	World Wide Web Consortium