Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI für Webbrowser

nach § 8 Absatz 1 Satz 1 BSIG – Version 3.0 vom 19.02.2024

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	20.03.2017	Erste Veröffentlichung des Mindeststandards
2.0	19.09.2019	Major Release – umfassende Überarbeitung
2.1	25.06.2020	Minor Release – Anpassungen und Konkretisierungen
3.0	19.02.2024	Major Release – Erweiterung des Scopes auf mobile Browser

Tabelle 1: Versionsgeschichte des Mindeststandards für Webbrowser. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/MST-Browser-Log

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

Risiken für die Cyber- und Informationssicherheit sind nicht zuletzt aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen allgegenwärtig. Dadurch betreffen potenzielle Schwachstellen und Cyberangriffe in der Regel nicht nur einzelne Stellen.

Umso wichtiger ist die Vorgabe verbindlicher Sicherheitsanforderungen an die Informationstechnik des Bundes. So kann ein einheitliches Mindestsicherheitsniveau mit effektiven Maßnahmen zur Abwehr von Cyberangriffen innerhalb der heterogenen Behördenlandschaft etabliert werden

Dazu legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes[1] fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards somit ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP Bund 2017)[2] eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Stellen des Bundes verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.

Die Mindeststandards richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe), Informationssicherheitsbeauftragte (ISB), IT-Betriebspersonal und Beschaffungsstellen. Die Gesamtverantwortung für die Informationssicherheit und damit auch für die Einhaltung der Mindeststandards trägt gemäß UP Bund 2017 die Leitung der jeweiligen Einrichtung[1].

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 dem Mindestsicherheitsniveau 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.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Einrichtung 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 Einrichtungen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Die von den Mindeststandards adressierten Stellen werden in § 8 Absatz 1 BSI-Gesetz (BSIG) definiert (siehe https://www.gesetze-im-internet.de/bsig_2009/__8.html). Zur besseren Lesbarkeit wird im weiteren Verlauf für alle dort genannten Stellen der Begriff „Einrichtung“ verwendet.
[2] Vgl. UP Bund (BMI 2017)
[3] Siehe FAQ zu den MST: https://www.bsi.bund.de/dok/MST-FAQ

Inhalt

1 Beschreibung

Webbrowser 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 Webbrowsers werden Daten in der Regel auch aus nicht vertrauenswürdigen Quellen geladen. Diese Daten können schädlichen Code (Viren, Trojaner, Spyware etc.) enthalten und das System 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 Webbrowsern grundsätzlich ein Risiko dar.

1.1 Einleitung und Abgrenzung

Durch die Umsetzung und Einhaltung dieses Mindeststandards sollen Risiken beim Einsatz von Webbrowsern minimiert werden. Das vorliegende Dokument beschreibt Sicherheitsanforderungen sowohl an Webbrowser, die auf Arbeitsplatzrechnern der Bundesverwaltung eingesetzt werden (im Folgenden kurz als Desktop-Browser bezeichnet), als auch an Webbrowser-Apps, die auf mobilen Plattformen wie Android oder iOS eingesetzt werden (im Folgenden kurz als mobile Browser bezeichnet). Mobile Browser bestehen technologiebedingt meist aus einer Anzeigekomponente in der App und einer Rendering-Engine, die mit dem Betriebssystem ausgeliefert wird. Die Rendering-Engine muss bei einigen mobilen Betriebssystemen zwingend verwendet werden (auch von Apps Dritter). Diese Aufspaltung führt dazu, dass Sicherheitsanforderungen des Mindeststandards bei mobilen Webbrowsern teilweise über Eigenschaften des Betriebssystems umgesetzt werden müssen oder gar nicht umgesetzt werden können. Da mobile Plattformen jedoch mit einem integrierten Browser in ihrer Distribution ausgeliefert werden, entfällt für sie die Abgrenzung zwischen Betriebssystem und App. Durch zentral gepflegte Komponenten profitieren auch andere Browserherstellende direkt von der Umsetzung der Forderungen durch die mobilen Plattformen. Weitere spezielle Hinweise befinden sich in den betroffenen Anforderungen.

Webbrowser, die ausschließlich auf interne Netze zugreifen können, sind nicht Gegenstand dieses Mindeststandards.

Bedarfsträger mit hohem oder sehr hohem Schutzbedarf können erweiterte Lösungen zur Absicherung nutzen. 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 Webbrowsers 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 Webbrowsers ist daher zu prüfen, ob die in Kapitel 2.1 und 2.2 aufgeführten Sicherheitsanforderungen an Browser und Entwicklung vollständig durch die Anbietenden implementiert und umgesetzt sind. Dabei haben Anbietende zu belegen (z. B. anhand einer Produktdokumentation), ob und wie ihre Produkte die

[4] Vgl. IT-Grundschutz-Kompendium (BSI 2023a), APP.1.2 Webbrowser

[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 Webbrowsern zu erweitern.

[6] Vgl. BSI-Empfehlung für sichere Web-Browser (BSI 2020), S. 1f

[7] Vgl. Sichere Inter-Netzwerk Architektur SINA (BSI 2016), S. 25f

[8] Vgl. Common Criteria Protection Profile for Remote-Controlled Browsers System (BSI 2008)
Für eine Übersicht zu diesen und weiteren Absicherungsmöglichkeiten vgl. auch BSI-CS 047 – Absicherungsmöglichkeiten beim Einsatz von Web-Browsern (BSI 2018), https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_047.pdf

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 Webbrowser nicht schon im Auslieferungszustand alle Anforderungen erfüllen muss. Es muss jedoch die Möglichkeit bestehen, ihnen über organisatorischer Maßnahmen, Konfiguration oder durch Erweiterungen gerecht zu werden. In zentral verwalteten Umgebungen können auch entsprechend geeignete und dokumentierte zentrale Sicherheits- und Überwachungslösungen bestimmte Sicherheitsanforderungen abdecken.

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2022[12].

MUSS / DARF NUR

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

DARF NICHT / DARF KEIN

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

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit 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. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

[9] Eine Abgleichstabelle zwischen den Mindestanforderungen und den für die Bundesverwaltung relevantesten Webbrowsern wird nach Veröffentlichung des Mindeststandards auf https://bsi.bund.de/mindeststandards unter „Webbrowser“ zur Verfügung stehen.
[10] Vgl. BSI-Standard 200-2 (BSI 2017, S. 18)
[11] Vgl. Key words for use in RFCs (IETF 1997)
[12] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2022)

2 Sicherheitsanforderungen

Die Sicherheitsanforderungen an Webbrowser sind im Folgenden in drei Unterkapitel gegliedert. Unterkapitel 2.1 beschreibt funktionale bzw. technische Voraussetzungen an das Softwareprodukt Webbrowser. Sie müssen bereits bei der Auswahl eines geeigneten Webbrowsers durch die jeweilige Einrichtung berücksichtigt werden. Unterkapitel 2.2 stellt organisatorische Sicherheitsanforderungen auf, die Anbietende im Rahmen von Entwicklung und Wartung des Webbrowsers erfüllen müssen. Unterkapitel 2.3 richtet sich an den Betrieb der Einrichtung, die den Mindeststandard umsetzt. Hier werden Prozesse, die Administration und Konfiguration von Webbrowsern geregelt.

2.1 Technische Sicherheitsanforderungen an Anbietende und Produkt

Im folgenden Unterkapitel geht es um funktionale bzw. technische Voraussetzungen, die der Webbrowser mitbringen muss, um einen mindeststandardkonformen Einsatz zu ermöglichen. Sie müssen bereits bei der Entwicklung des Webbrowsers umgesetzt werden. Die konkrete Konfiguration verfügbarer Optionen ist dagegen Aufgabe des Betriebs der jeweiligen Einrichtung und wird in Unterkapitel 2.3 gebündelt beschrieben.

WB.2.1.01 – Vertrauenswürdige Kommunikation

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

b) Der Webbrowser MUSS folgende Anforderungen an Zertifikate und deren Überprüfung erfüllen:

- Zertifikate MÜSSEN gemäß dem X.509-Standard[14] unterstützt werden.
- Eine Liste von Wurzelzertifikaten allgemein anerkannter Zertifizierungsstellen (Certification Authority; CA-Zertifikate) MUSS aktualisiert bereitgestellt werden.[15]
- Der Webbrowser 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 umfasst mindestens die Prüfung der zeitlichen Gültigkeit jedes Zertifikats einer Zertifikatskette und die Prüfung des Sperrstatus dieser Zertifikate (z. B. mittels Certification Revocation List (CRL) oder Online Certificate Status Protocol (OCSP))[16] sowie die Prüfung aller Signaturen dieser Zertifikate (letzteres ggf. nicht bei Wurzelzertifikaten, die keine Signatur tragen.
- Eigene Zertifikate MÜSSEN dem Zertifikatsspeicher zugefügt werden können.
- Jeglichen Zertifikaten MUSS lokal das Vertrauen entzogen werden können.
- Der schreibende Zugriff auf den Zertifikatsspeicher DARF NUR mit administrativen Rechten oder mit der expliziten Zustimmung des Benutzenden erfolgen.

[13] Der Mindeststandard TLS fordert aktuell den Einsatz von TLS mindestens in der Version 1.2 in Kombination mit Perfect Forward Secrecy (PFS). Vgl. Mindeststandards TLS (BSI 2023b)

[14] Vgl. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (IETF 2008) sowie IETF (2014).

[15] Als Orientierung kann bspw. die Common CA Database (https://www.ccadb.org/) genutzt werden.

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

c) Der Webbrowser MUSS die Kommunikationsform geeignet und nicht manipulierbar darstellen.[17]

- Den Benutzenden MUSS angezeigt werden, ob die Kommunikation mit dem Webserver verschlüsselt oder im Klartext bzw. gemischt erfolgt (beispielsweise durch Symbole, farbliche Hervorhebungen oder Anzeige der Protokolle wie „http“ oder „https“). Bei gemischten Inhalten MUSS die Ausführung unverschlüsselt übertragener aktiver Inhalte konfigurierbar oder standardmäßig deaktiviert sein.
- Den Benutzenden MUSS ein fehlendes CA-Zertifikat im Zertifikatsspeicher oder ein ungültiges/widerrufenes X.509-Zertifikaten des Web-Servers als Prüfergebnis signalisiert werden. Die verschlüsselte Verbindung DARF dann NICHT ohne explizite Bestätigung durch die Benutzenden aufgebaut werden.
- Es MUSS den Benutzenden möglich sein, sich die URL der aktuell angezeigten Webseite vollständig anzeigen zu lassen.

d) Der Webbrowser MUSS HTTP Strict Transport Security (HSTS) unterstützen. Die Implementierung SOLLTE RFC 6797[18] entsprechen, abweichende Implementierungen zum Schutz der Benutzenden vor Tracking sind jedoch zulässig, sofern sie die gleichen Sicherheitsziele erreichen.

WB.2.1.02 – Updates

a) Es MUSS Update-Mechanismen geben, durch die der Webbrowser automatisch aktualisiert wird.

b) Updates DÜRFEN NUR dann eingespielt werden, wenn zuvor durch den Update-Mechanismus eine Integritätsprüfung durchgeführt wurde und diese ein positives Prüfergebnis liefert. Nicht korrekte Prüfergebnisse MÜSSEN geeignet signalisiert werden.

WB.2.1.03 – Schutz vertrauenswürdiger Daten

a) Der Webbrowser MUSS folgende Einstellungen für Cookies bereitstellen:

- Das Anlegen und Auslesen von Cookies MUSS auf Anforderung der Benutzenden oder durch die zentrale Administration deaktiviert werden können.
- Bereits angelegte Cookies MÜSSEN auf Anforderung der Benutzenden oder durch die zentrale Administration gelöscht werden können.
- Das Anlegen und Auslesen von Cookies durch Dritte MUSS standardmäßig blockiert sein oder auf Anforderung der Benutzenden oder durch die zentrale Administration blockiert werden können.

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

- Website-Daten sowie der Browser-Cache MÜSSEN auf Anforderung der Benutzenden oder durch die zentrale Administration gelöscht werden können.
- Der Browserverlauf und die Liste der Auto-Vervollständigungen MÜSSEN auf Anforderung der Benutzenden oder durch die zentrale Administration gelöscht werden können.
- Funktionalitäten zur Auto-Vervollständigung (Name, E-Mail, usw.) MÜSSEN auf Anforderung der Benutzenden oder durch die zentrale Administration deaktiviert werden können.

c) Es MUSS möglich sein, Zugriffe auf Kamera, Mikrofon und Standort NUR nach expliziter Zustimmung durch die Benutzenden zu erlauben.

[17] 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. Hinweis: Derzeit findet eine Revision der EU 910/2014 ("eIDAS-Verordnung") statt. Die veröffentlichten Entwürfe sehen vor, dass die in qualifizierten Webseitenzertifikaten (QWAC) enthaltenen Identitätsinformationen durch Browser in einer nutzerfreundlichen Art und Weise angezeigt werden müssen. Allgemein ist es empfehlenswert, solche in Extended-Validation-Zertifikaten (insbesondere aus QWACs) enthaltenen Identitätsinformationen durch Browser transparent darzustellen.

[18] Vgl. HTTP Strict Transport Security (IETF 2012)

d) Die Übertragung von Telemetriedaten[19] MUSS konfiguriert und deaktiviert werden können. Die Einstellung SOLLTE durch die Administration zentral vorgegeben werden können, so dass Benutzende diese nicht verändern können. Falls dies nicht möglich ist (z. B. bei mobilen Browsern), MÜSSEN Benutzende durch die Einrichtung verpflichtet werden, die Basiskonfiguration nicht zu verändern.

e) Es MUSS möglich sein, eine kontextfreie Browserinstanz auszuführen („Inkognito-“ oder „privater Modus“), die keine zuvor gespeicherten Daten (Cookies, Website-Daten, Cache, Download-Chronik) berücksichtigt sowie während der Sitzung anfallende Daten nach Beenden dieser Browserinstanz wieder löscht.

WB.2.1.04 – Externe Dienste

Die Kommunikation mit externen Diensten[20] MUSS deaktiviert sein oder durch die Administration deaktiviert werden können.

Dies betrifft zum Beispiel:

- adress- oder inhaltsbasierte Schutzmechanismen
- Web- oder Cache-Proxies (bspw. Mini-Browser)

WB.2.1.05 – Same-Origin-Policy

Die Same-Origin-Policy MUSS umgesetzt sein.[21] Insbesondere DÜRFEN Ressourcen nicht zwischen Webseiten unterschiedlicher Herkunft geteilt werden. 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 möglich sein, wenn die Parameter in ihrer URL mit denen der Webseite übereinstimmen oder die Berechtigung explizit mittels Cross-Origin Resource Sharing (CORS) erlaubt ist.[22]

WB.2.1.06 – Sichere Konfiguration

a) Eine Oberfläche für die Verwaltung der Einstellungen MUSS bereitstehen. Einstellungen, die nicht über diese Oberfläche konfigurierbar sind, MÜSSEN bei Auslieferung des Webbrowsers bereits standardmäßig den Anforderungen des Mindeststandards entsprechen. Einstellungen, um Erweiterungen (falls verfügbar) und JavaScript aktivieren und deaktivieren zu können, MÜSSEN vorhanden sein.

b) Die unter WB.2.3.04 geforderte Basiskonfiguration MUSS zentral anwendbar sein oder durch die mit dem Webbrowser ausgelieferte Standardkonfiguration erfüllt sein.

c) Änderungen an der Basiskonfiguration über die grafische Bedienoberfläche SOLLTE verhindert werden können. Falls dies nicht möglich ist (z.B. bei mobilen Browsern), MÜSSEN Benutzende durch die Einrichtung verpflichtet werden, die Basiskonfiguration nicht zu verändern.

d) Sofern eine Synchronisation mit externen Speicherdiensten und -orten (sog. Cloud-Dienste) vorhanden ist, MUSS diese zentral durch die Administration deaktivierbar sein.[23]

e) Alternative Protokolle zur Auflösung von DNS-Anfragen (z.B. DNS over HTTPS (DoH) oder DNS over TLS (DoT)) MÜSSEN deaktivierbar sein.

[19] Unter dem Begriff *Telemetriedaten* werden alle Daten (Nutzer- und Nutzungsdaten, Systemdaten) zusammengefasst, die ein Hersteller auf einem Gerät erhebt, um seine Produkte weiterzuentwickeln.
[20] *Externe Dienste* im Sinne dieses Mindeststandards meint Dienste, die außerhalb der internen Netze der Einrichtung (z. B. außerhalb der Netze des Bundes (NdB)) kommunizieren. Update-Dienste der Browserherstellenden gem. WB.2.1.02 sind ausgenommen.
[21] Vgl. Same-origin policy (Mozilla 2024a)
[22] Vgl. CORS (Mozilla 2024b)
[23] Plattformbedingt sind Synchronisationsmechanismen ggf. nur systemweit konfigurierbar.

WB.2.1.07 – Minimale Rechte

Der Webbrowser MUSS nach seiner Initialisierung mit minimal möglichen Rechten im Betriebssystem ablaufen. Bei der Initialisierung darf der Webbrowser mit erweiterten Rechten laufen, diese MUSS er aber danach wieder abtreten.

WB.2.1.08 – Sandboxing und Kapselung

a) Die Architektur des Webbrowsers MUSS die folgenden Eigenschaften besitzen:

- Sämtliche Komponenten MÜSSEN voneinander und zum Betriebssystem hin gekapselt sein.
- Darstellungskomponenten MÜSSEN von Steuerungskomponenten gekapselt sein.

b) Webseiten einschließlich ihrer Darstellungskomponenten MÜSSEN grundsätzlich in Form eigenständiger Prozesse voneinander isoliert werden. Zugriffe zwischen Webseiten MÜSSEN vom Webbrowser kontrolliert erfolgen

WB.2.1.09 – Content Security Policy (CSP)

Der Webbrowser MUSS die Content Security Policy mindestens in Level 2.0 (CSP 2.0) gemäß den W3C-Spezifikationen[24] umsetzen. Die Implementierung DARF in Ausnahmefällen von den W3C-Spezifikationen abweichen, falls der Webbrowser selbst strengere Maßnahmen umsetzt.

WB.2.1.10 – Subresource Integrity

Der Webbrowser MUSS Subresource Integrity (SRI)[25] gemäß den W3C-Spezifikationen umsetzen.

2.2 Organisatorische Sicherheitsanforderungen an Anbietende und Produkt

Die folgenden organisatorischen Sicherheitsanforderungen haben Anbietende im Rahmen von Entwicklung und Wartung des Webbrowsers zu gewährleisten.

WB.2.2.01 – Entwicklung

Es DÜRFEN NUR Programmiersprachen und -werkzeuge verwendet werden, die Mechanismen zum Stack- und Heapschutz implementieren. Beim Erstellen des Webbrowsers MÜSSEN diese Mechanismen genutzt werden. Der Webbrowser MUSS die vom Betriebssystem bereitgestellten Speicherschutzmechanismen nutzen.

WB.2.2.02 – Aktualisierung

Es MÜSSEN Sicherheitsupdates für den Webbrowser und seine Komponenten durch die Herstellenden bereitgestellt werden. Je nach Plattform erfolgt die Bereitstellung der Sicherheitsupdates zusammen mit Updates für die Plattform selbst. Bei kritischen Schwachstellen[26] SOLLTE ein Update innerhalb von 28 Tagen, nachdem die Schwachstelle öffentlich bekannt wurde, bereitgestellt werden. Wird die Schwachstelle bereits öffentlich ausgenutzt, MÜSSEN Updates spätestens nach 7 Tagen bereitgestellt werden.

WB.2.2.03 – Kontaktmöglichkeit

Um potenzielle Schwachstellen melden zu können, MÜSSEN seitens der Anbietenden Kontaktmöglichkeiten für Sicherheitsmeldungen bereitgestellt werden.

[24] Vgl. Content Security Policy Level 2 (W3C 2016a). CSP Level 3.0 ist derzeit in Erarbeitung, befindet sich jedoch noch im *Draft*-Status.
[25] Vgl. Subresource Integrity (W3C 2016b)
[26] Eine Schwachstelle wird als kritisch bezeichnet, wenn sie nach dem Industriestandard Common Vulnerability Scoring System (CVSS) v3.1 als *Critical* (9.0 - 10.0) bewertet wird (vgl. FIRST 2019).

WB.2.2.04 – Dokumentation

Funktionen, insbesondere zur Telemetrie, die auf dem IT-System gespeicherte Daten verändern oder exfiltrieren können, MÜSSEN transparent, sach- und bedarfsgerecht dokumentiert sein.[27]

2.3 Sicherheitsanforderungen an den Betrieb

Die Wirksamkeit von Sicherheitsmechanismen ist neben den bereits aufgeführten Sicherheitsanforderungen ebenso im Kontext des Betriebs eines Webbrowsers zu betrachten. Daher müssen die im Folgenden aufgeführten Sicherheitsanforderungen durch den Betrieb der Einrichtung umgesetzt werden. Sie beinhalten auch die Konfiguration von Einstellungsmöglichkeiten, die in Unterkapitel 2.1 als technische Voraussetzung gefordert werden.

WB.2.3.01 – Betriebssystem

Das Betriebssystem des Arbeitsplatzrechners MUSS dem Webbrowser 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.

WB.2.3.02 – Administration

a) Es MUSS ein Prozess zur Verwaltung von Zertifikaten vorgehalten werden (siehe WB.2.1.01b).[28]

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

c) Es MUSS ein Prozess für die Verwaltung der Konfiguration vorgehalten werden (siehe WB.2.1.06), falls die Basiskonfiguration WB.2.3.04 nicht in der Standardkonfiguration umgesetzt wird.

WB.2.3.03 – Erweiterungen

Die Installation von Erweiterungen auf Arbeitsplatz-PCs MUSS durch Vorgaben geregelt sein und SOLLTE zentral verwaltet werden. Den Benutzenden SOLLTE NUR die Installation von Erweiterungen einer zentralen Whitelist erlaubt werden. Da im mobilen Bereich weniger Erweiterungen vorhanden sind und auch keine direkte Installation aus beliebigen Quellen möglich ist, kann die erlaubte Nutzung auch organisatorisch geregelt werden.

Darüber hinaus stellt der vorliegende Mindeststandard für Webbrowser keine Anforderungen an Erweiterungen auf, da diese wie andere Software auch im Rahmen des Informationssicherheits-managements der Einrichtung zu behandeln sind. Insbesondere gelten die Anforderungen des IT-Grundschutz-Bausteins „APP.6 Allgemeine Software“[29] auch für Webbrowser-Erweiterungen.

WB.2.3.04 – Basiskonfiguration

Die Einrichtung MUSS den Webbrowser in folgender Basiskonfiguration ausliefern:

a) Das Protokoll TLS MUSS gemäß dem Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)[30] aktiviert sein.

b) Es MUSS geprüft werden, ob die Liste der Root-CAs eingeschränkt werden muss. Kriterien zur Vertrauenswürdigkeit der Zertifizierungsstellen finden sich in der TR-03116-4.[31] In Bezug auf die

[27] Art und Umfang der Dokumentation müssen dem Informationsbedarf des zuständigen Fachpersonals genügen. Insbesondere sollten IT-SiBe in die Lage versetzt werden, die Auswirkungen der Funktionen auf die Informationssicherheit zu bewerten.

[28] Ggf. sind die vom Webbrowser genutzten Zertifikate im Zertifikatsspeicher des Betriebssystems gespeichert.

[29] Vgl. IT-Grundschutz-Kompendium, APP.6 Allgemeine Software (BSI 2023a)

[30] Vgl. Mindeststandards TLS (BSI 2023b)

[31] Vgl. TR-03116-4 (BSI 2023c)

Eingriffsrechte Dritter SOLLTEN insbesondere Aussteller aus Staaten mit besonderen Sicherheitsrisiken[32] kritisch geprüft werden.

c) Die Nutzung von HSTS MUSS für alle Webseiten aktiviert sein. Abweichungen bei Vorliegen besonderer Geheim- und Datenschutzanforderungen sind möglich.[33]

d) Cookies Dritter DÜRFEN NICHT vom Webbrowser akzeptiert werden.

e) In den Netzen des Bundes DARF NUR der interne DNS-Resolver der Einrichtung für die DNS-Auflösung des Webbrowsers genutzt werden.[34]

f) Encrypted Media Extensions (EME)[35] MÜSSEN deaktiviert werden, wenn diese nicht benötigt werden.

g) Funktionen zur Auto-Vervollständigung MÜSSEN deaktiviert sein. Eine Ausnahme besteht für Passwortmanager, sofern sie die Anforderungen aus WB.2.3.06 erfüllen.

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

i) Der Zugriff auf Kamera, Mikrofon und Standort DARF NICHT ohne explizite Zustimmung der Benutzenden erfolgen.

j) Die vorhandenen integrierten Darstellungsmechanismen des Webbrowsers (z. B. für PDF) MÜSSEN aktiviert sein und bevorzugt verwendet werden.

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

l) Die Synchronisation von schützenswerten Daten (Anmeldeinformationen, Cookies, Chronik, privaten Zertifikaten, Lesezeichen, Cache) mit externen Speicherdiensten (z. B. Cloud) MUSS deaktiviert sein.

m) Zentral vorgegebene Konfigurationen SOLLTEN vor Änderungen durch Benutzende geschützt sein. Falls dies nicht möglich ist (z. B. bei mobilen Browsern), MÜSSEN Benutzende durch die Einrichtung verpflichtet werden, die Basiskonfiguration nicht zu verändern.

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

o) Der Zugriff auf Browserfunktionen und Daten durch digitale Sprachassistenzsysteme SOLLTE deaktiviert werden.

WB.2.3.05 – Überprüfung auf schädliche Inhalte

Es MÜSSEN Schutzmechanismen wie z. B. Content-Filter eingesetzt werden, die vor dem Aufruf als schädlich eingestufter Webseiten warnen.[36]

---

[32] Vgl. Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 SÜG und § 32 SÜG (BMI 2020)

[33] Da HSTS zum Tracken der Benutzenden 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.

[34] Vgl. IT-Grundschutz-Kompendium (BSI 2023a), APP.1.2.A13 Nutzung von DNS-over-HTTPS

[35] Vgl. Encrypted Media Extensions (W3C 2017)

[36] Das BSI betreibt ein zentrales Schadsoftware-Präventions-System (SPS) für die Netze des Bundes (NdB). Es fungiert als kontinuierlich gepflegte Blacklist, so dass die Anforderung für angeschlossene Einrichtungen grundsätzlich erfüllt ist. Dennoch sollte geprüft werden, ob zusätzliche, individuelle Maßnahmen notwendig sind.
Bei integrierten inhalts- und adressbasierten Schutzmechanismen des Webbrowsers ist darauf zu achten, dass die Überprüfung der Webseite lokal erfolgt und nicht durch externe Dienste (siehe WB.2.1.04 und WB.2.3.04 j).

WB.2.3.06 – Passwortmanager

a) Browsereigene Passwortmanager erfüllen in der Regel nicht die Anforderungen an die Informationssicherheit. Es SOLLTEN daher externe Passwortmanager genutzt werden, die den Anforderungen der Organisation entsprechen.

b) Wird dennoch der browsereigene Passwortmanager genutzt, MÜSSEN folgende Sicherheitsanforderungen erfüllt sein:

- Eine direkte und eindeutige Beziehung zwischen Webseite (URL) und hierfür gespeichertem Passwort MUSS zuverlässig möglich sein.
- Passwörter MÜSSEN vor Zugriffen außerhalb des Webbrowsers geschützt werden.
- Bei Desktop-Webbrowsern MUSS dazu der Zugriff auf gespeicherte Passwörter durch ein Hauptpasswort effektiv geschützt und bei jeder neuen Browser-Sitzung eine erneute Autorisierung eingefordert werden. Das Hauptpasswort MUSS dann den verbindlichen Vorgaben der Behörde entsprechen.[37] Bei mobilen Webbrowsern ist der Zugriff auf die gespeicherten Passwörter durch die App-Sandbox geschützt, so dass auf einen zusätzlichen Zugriffsschutz verzichtet werden kann.
- Bereits gespeicherte Passwörter und das Hauptpasswort MÜSSEN auf Anforderung der Benutzenden gelöscht werden können.

WB.2.3.07 – Updates/Patches

a) Der Betrieb MUSS Updates nach WB.2.2.02 unverzüglich einspielen.

b) Unabhängig von der Verfügbarkeit eines Updates MUSS der Betrieb spätestens 7 Tage nach Bekanntwerden einer kritischen Schwachstelle[38] Maßnahmen zur Mitigation umgesetzt haben. Dies kann bspw. im Rahmen der vom BSI empfohlenen Zwei-Browser-Strategie[39] für Desktop-Webbrowser die zwischenzeitliche Abschaltung des betroffenen Browsers bedeuten.

c) Falls für den verwendeten Webbrowser keine Sicherheitsupdates mehr zur Verfügung gestellt werden, MUSS gemäß UP Bund[40] schnellstmöglich eine Umstellung auf einen neuen Webbrowser erfolgen. Dies MUSS regelmäßig (mindestens jährlich) vorausschauend geprüft werden.

[37] Vgl. IT-Grundschutz-Kompendium, ORP.4.A8 Regelung des Passwortgebrauchs (BSI 2023a)
[38] Eine Schwachstelle wird als kritisch bezeichnet, wenn sie nach dem Industriestandard Common Vulnerability Scoring System (CVSS) v3.1 mit *Critical* (9.0 - 10.0) bewertet wird (vgl. FIRST 2019).
[39] Vgl. IT-Grundschutz-Kompendium, APP.1.2.A12 Zwei-Browser-Strategie (BSI 2023a)
[40] Vgl. Umsetzungsplan Bund (BMI 2017), Kapitel 7.2

Literaturverzeichnis

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

BMI (2020) Bundesministerium des Innern und für Heimat: Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 SÜG und § 32 SÜG, 24.01.2020

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: Common Criteria Protection Profile for Remote-Controlled Browser System (ReCoBS), BSI-PP-0040, Version 1.0, 2008, https://www.bsi.bund.de/dok/403490

BSI (2016) Bundesamt für Sicherheit in der Informationstechnik: Sichere Inter-Netzwerk Architektur SINA, BSI-BRO16/322, 2016, https://www.bsi.bund.de/dok/6603822

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, 2017, https://www.bsi.bund.de/dok/10027846

BSI (2018) Bundesamt für Sicherheit in der Informationstechnik: Absicherungsmöglichkeiten beim Einsatz von Web-Browsern, BSI-CS 047, Version 2.0 vom 11.07.2018, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_047.pdf

BSI (2020) Bundesamt für Sicherheit in der Informationstechnik: BSI-Empfehlung für sichere Web-Browser, BSI-CS 071, Version 2.0 vom 13.01.2020, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_071.html

BSI (2024a) Bundesamt für Sicherheit in der Informationstechnik: Änderungsübersicht zum Mindeststandard des BSI für Webbrowser, https://www.bsi.bund.de/dok/MST-Browser-Log

BSI (2024b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/MST-FAQ

BSI (2023a) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Edition 2023, https://www.bsi.bund.de/dok/1073656

BSI (2023b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 zur Verwendung von Transport Layer Security, Version 2.4 vom 25.05.2023, https://www.bsi.bund.de/dok/MST-TLS

BSI (2023c) Bundesamt für Sicherheit in der Informationstechnik: TR 03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, 07.03.2023, https://www.bsi.bund.de/dok/6615234

DIN (2022) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2022-12, 2022

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

Mozilla (2024a) Mozilla: Same-origin policy, https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy, abgerufen am 25.01.2024

Mozilla (2024b) Mozilla: Cross-Origin Resource Sharing (CORS), https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS, abgerufen am 25.01.2024

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 16.03.2020

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 05.10.2022

IETF (2012) Internet Engineering Task Force: HTTP Strict Transport Security (HSTS), RFC 6797, https://tools.ietf.org/html/rfc6797, abgerufen am 16.03.2020

IETF (2014) Internet Engineering Task Force: Updates to the Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, RFC 6818, https://www.rfc-editor.org/rfc/rfc6818, abgerufen am 05.10.2022

W3C (2016a) World Wide Web Consortium: Content Security Policy Level 2, 2016, https://www.w3.org/TR/CSP2/, abgerufen am 16.03.2020

W3C (2016b) World Wide Web Consortium: Subresource Integrity, 2016, https://www.w3.org/TR/SRI/, abgerufen am 16.03.2020

W3C (2017) World Wide Web Consortium: Encrypted Media Extensions, 2016, https://www.w3.org/TR/encrypted-media/, abgerufen am 16.03.2020

Abkürzungsverzeichnis

ASLR	Address Space Layout Randomization
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CORS	Cross-Origin Resource Sharing
CPT	Certification Path Validation Test Tool
CRL	Certificate Revocation List
CSP	Content Security Policy
CVSS	Common Vulnerability Scoring System
DEP	Data Execution Prevention
DIN	Deutsches Institut für Normung
DNS	Domain Name System
DoH	DNS over HTTPS
DoT	DNS over TLS
EME	Encrypted Media Extensions
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IETF	Internet Engineering Task Force
IT	Informationstechnik
MST	Mindeststandard
NdB	Netze des Bundes
NX	No-execute
OCSP	Online Certificate Status Protocol
OS	Operating System
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
UP Bund	Umsetzungsplan Bund

W3C	World Wide Web Consortium