Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI für sichere Web-Browser

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 20.03.2017

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

§ 8 Absatz 1 BSIG regelt die Befugnis des BSI, allgemeine technische Mindeststandards für die Sicherung der Informationstechnik des Bundes festzulegen. Ein Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um einen angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen.

Mindeststandards sind Vorgaben des BSI für die Stellen des Bundes. Allerdings kann das BMI im Benehmen mit dem IT-Rat die dort formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Stellen des Bundes als verbindlich erklären.[1] Darüber hinaus kann der IT-Planungsrat Mindeststandards in Teilen oder als Ganzes als gemeinsame Standards für den zur Aufgabenerfüllung zwischen dem Bund und den Ländern notwendigen Datenaustausch festlegen.[2]

Über die Bundesverwaltung hinaus sind Mindeststandards nach § 8 Absatz 1 BSIG auch in der öffentlichen Verwaltung der Länder und Kommunen für den Einsatz von Informationstechnik und zur Sicherung Kritischer Infrastrukturen von grundsätzlicher Bedeutung. Ziele, Anforderungen und Empfehlungen von Mindeststandards können dazu genutzt werden, eigene Sicherheitsanforderungen anzupassen oder zu überprüfen, auch bei der Erstellung von Leistungsbeschreibungen im Rahmen eigener Vergabeverfahren. Anbieter von Informationstechnik und IT-Dienstleister können Mindeststandards dazu nutzen, ihre angebotenen Produkte sicherer zu machen.

1 vgl. § 8 Absatz 1 Satz 2 BSIG

2 Grundlage hierfür sind Artikel 91c GG und § 3 Absatz 1 des Vertrages zur Ausführung des Artikel 91c GG zwischen dem Bund und den Bundesländern vom 01.04.2010.

1 Einordnung und Begründung

Dieser Mindeststandard beschreibt Sicherheitsanforderungen an einen Web-Browser, der auf Arbeitsplatzrechnern der Bundesverwaltung eingesetzt wird. Diese Anforderungen sind zum Erreichen eines Mindestmaßes an Informationssicherheit einzuhalten.

1.1 Kurzbeschreibung

Web-Browser dienen dem Abruf und der Darstellung von Daten aus dem Internet, wie beispielsweise Hypertext, Dokumenten, Bildern, Video-, Audio- und andere Formaten.[3] Die Nutzung von Zusatzfunktionalitäten (z. B. Darstellung bestimmter Medienformate) erfordert häufig die Einbindung weiterer Darstellungskomponenten (Plug-ins) beziehungsweise die Nutzung externer Bibliotheken des Betriebssystems oder dritter Parteien.

1.2 Begründung Handlungsbedarf und Sicherheitsniveau

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. Dies kann zum Verlust der Verfügbarkeit, Vertraulichkeit und Integrität von schützenswerten Daten führen. Somit stellt eine Nutzung von Web-Browsern erst einmal ein Risiko dar. Durch die Umsetzung und Einhaltung dieses Mindeststandards sollen diese Risiken minimiert werden.

Dieser Mindeststandard gilt für normalen Schutzbedarf.[4] Ab dem Schutzbedarf hoch oder bei über diesen Mindeststandard hinausgehenden Bedrohungen (siehe Kapitel 3), sind weitere Anforderungen auf Basis einer Risikoanalyse zu berücksichtigen, die nicht Bestandteil dieses Mindeststandards sind.

Bedarfsträgern mit hohem oder sehr hohem Schutzbedarf wird der Einsatz erweiterter Lösungen empfohlen. Dazu gehören insbesondere virtualisierte Systeme[5] oder auch Remote-Controlled-Browser-Umgebungen.[6]

1.3 Abgrenzung

Gegenstand dieses Mindeststandards sind Web-Browser auf Arbeitsplatzrechnern von Stellen des Bundes im Sinne des § 8 Absatz 1 BSIG. Web-Browser, die auf mobilen Plattformen wie Android oder iOS eingesetzt werden oder nur ausschließlich auf sichere, interne Netzwerke zugreifen können, sind nicht Gegenstand dieses Mindeststandards.

Die Sicherheitsanforderungen (siehe Kapitel 4) beziehen sich auf Konfiguration, Auslieferungszustand und Darstellungskomponenten des Web-Browsers sowie auf Interaktionen mit der Betriebssystemumgebung.

Weiterführende Aspekte, wie etwa die sichere Entwicklung von Software zur Fehlerreduktion oder die Vertrauenswürdigkeit von Zertifikaten bedürfen einer vertieften Prüfung. In diesem Zusammenhang wird idealerweise der Dialog mit Anbietern von Web-Browsern gesucht.

3 vgl. BSI (2014), S. 4225f.
4 vgl. BSI (2014), S. 77
5 vgl. BSI (2013), S. 25f.
6 vgl. BSI (2008), S. 1ff.

2 Methode und Anwendung

Die hier aufgeführten Anforderungen an die Sicherheit basieren auf Normen, Standards und Richtlinien. Darüber hinaus können weitere Regelungen vorgegeben werden.

Die Auswahl der Sicherheitsanforderungen erfolgt in drei Schritten:

1. Analyse typischer Bedrohungen (siehe Kapitel 3) , gegen die Web-Browser bestehen müssen.
2. Ableiten funktionaler und organisatorische Sicherheitsanforderungen an Web-Browser (siehe Kapitel 4.2). Diese müssen anbieterseitig implementiert und umgesetzt sein, damit Web-Browser gegen typische Bedrohungen wirksam geschützt sind.
3. Aufstellen von Sicherheitsanforderungen für den Betrieb von Web-Browsern (siehe Kapitel 4.3), welche die Sicherheitseigenschaften stützen oder erweitern.

2.1 Zielgruppen

Dieser Mindeststandard richtet sich an IT-Verantwortliche, IT-Sicherheitsbeauftragte und IT-Fachkräfte, sowie die mit der Beschaffung beauftragten Stellen in der Bundesverwaltung.[7] Aber auch für Anbieter von Web-Browsern sowie weitere interessierte Personen kann dieser Mindeststandard zweckdienlich sein.

2.2 Umsetzung

Vor Einsatz eines Web-Browsers ist zu prüfen, ob die in Kapitel 4.2 aufgeführten „Sicherheitsanforderungen an die 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 an die Sicherheit erfüllen.

Eigene Überprüfungen in einer dem geplanten Einsatzszenario entsprechenden Umgebung werden ausdrücklich empfohlen (Laborumgebung). Abseits der Beschaffung selbst ist zu überprüfen, ob die Sicherheitsanforderungen an den Betrieb (siehe Kapitel 4.3) erfüllt sind.

2.3 Hinweis „zentral verwaltete Umgebungen“

Sicherheitsanforderungen an den Betrieb (siehe Kapitel 4.3) können in zentral verwalteten Umgebungen auch durch entsprechend geeignete und dokumentierte zentrale Sicherheits- und Überwachungslösungen erfüllt werden.

7 vgl. § 2 Absatz 3 BSIG

3 Bedrohungen

3.1 Verfügbarkeit, Vertraulichkeit und Integrität

Typische Bedrohungen für Web-Browser lassen sich in die sieben Kategorien „Schadprogramme“, „Abhören“, „Schwachstellen“, „Update-Integrität“, „Darstellung“, „Privatsphäre“ und „Administration“ aufgliedern. Diese Kategorien sind nachfolgend in Tabelle 1 dargestellt und näher beschrieben.

Kategorie	ID	Beschreibung
Schadprogramme	3.1.1	Ein Angreifer versucht, schädlichen Code mittels Web-Browser zu laden, um die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten auf dem Arbeitsplatzrechner oder angeschlossenen Netzen zu bedrohen.
Abhören	3.1.2	Ein Angreifer versucht, die Kommunikation zwischen Web-Browser und einem Web-Server zu belauschen.
Schwachstellen	3.1.3	Ein Angreifer versucht, eine ihm bekannte Schwachstelle des Web-Browsers oder einer von diesem vermittelten Ressource auszunutzen, um beispielsweise schädlichen Code auf den Arbeitsplatzrechner zu laden.
Update-Integrität	3.1.4	Ein Benutzer kann unwissentlich ein nicht integres Web-Browser-Update nutzen.
Darstellung	3.1.5	Der Web-Browser kann in einer Art und Weise benutzt werden, die unsicher ist, obwohl der Benutzer davon ausgeht, dass er den Web-Browser in einer sicheren Art und Weise nutzt. Ein Benutzer kann unwissentlich mit einer nicht sicheren Browser-Konfiguration arbeiten.
Privatsphäre	3.1.6	Vertrauenswürdige Daten eines Benutzers, insbesondere Passwörter, können zufällig oder böswillig unbefugten Dritten zugänglich sein.
Administration	3.1.7	Eine fehlerhafte Administration des Web-Browsers könnte zu einer unsicheren Konfiguration führen.

Tabelle 1: Darstellung und Beschreibung typischer Bedrohungen nach Kategorien

3.2 Spezifische Risikobetrachtung

Web-Browser haben mittlerweile eine enormen Funktionsvielfalt und erreichen zum Teil die Mächtigkeit moderner Betriebssysteme. Die damit einhergehende Komplexität bietet grundsätzlich ein hohes Potenzial an Sicherheitsproblemen. So sind immer wieder programmtechnische und konzeptionelle Schwachstellen zu verzeichnen, die in aller Regel vermeidbar wären, aber aufgrund von Komplexität und bestehenden Rahmenbedingungen trotzdem vorkommen. Hierbei handelt es sich nicht selten um gravierende Schwachstellen, die erhebliche Folgen für die Vertraulichkeit und Integrität der gespeicherten oder übertragenen Daten sowie die Verfügbarkeit des Gesamtsystems haben können. Dem gegenüber steht eine unüberschaubare Anzahl von Web-Servern, die durch Schadprogramme kompromittiert worden ist.

Daher sind Internetinhalte grundsätzlich als nicht vertrauenswürdig einzustufen und müssen jeweils individuell und wiederkehrend hinterfragt werden. Nur unter besonderen Voraussetzungen steigt der Grad der technischen Vertrauenswürdigkeit der geladenen Inhalte. Eine Unterscheidung zwischen

vertrauenswürdigen und nicht vertrauenswürdigen Inhalten ist oft nur noch in kontrollierten Bereichen möglich, etwa im Intranet einer Institution.

Schadprogramme (siehe ID 3.1.1) können als Teil von Werbe-Bannern, JavaScript- und ActionScript-Programmen oder auch als Bestandteil von PDF-Downloads über Web-Browser auf Arbeitsplatzrechner geladen werden. Nutzen so geladene Schadprogramme eine Schwachstelle (siehe ID 3.1.3) aus, ist ein erweiterter Zugang zum System und den dort gespeicherten Daten möglich. Gegebenenfalls lädt das erste Schadprogramm weitere Schadprogrammteile aus dem Internet nach. Anschließend können Daten von Dritten ausgespäht, manipuliert oder auch verschlüsselt werden (siehe ID 3.1.2).[8]

Ein wesentlicher Faktor des vorhandenen Gefahrenpotenzials liegt in der Aktualität und Pflege des jeweiligen Web-Browsers. So kann der Anbieter entscheidend dazu beitragen, dass die Ausnutzung von Schwachstellen (siehe ID 3.1.3) keine weite Verbreitung findet, indem er unverzüglich signierte Sicherheitsupdates bereitstellt. Im weiteren Verlauf hat der Betreiber dann dafür Sorge zu tragen, dass Sicherheitsupdates unter Beachtung seiner Sorgfaltspflichten (siehe ID 3.1.4) ebenso unverzüglich auf den Arbeitsplatzrechnern eingespielt werden.

Ein weiterer wesentlicher Faktor ist die Konfiguration der Browser-Einstellungen (siehe ID 3.1.5). Eine Speicherung von Cookies, Passwörtern, Verläufen, Formulardaten und Suchbegriffen erhöht zwar den Nutzerkomfort, aber auch die Gefahr, dass Daten von Dritten oder Schadprogrammen missbräuchlich ausgelesen werden (siehe ID 3.1.6). Die Aktivierung von Erweiterungen erhöht ebenfalls den Nutzerkomfort, vergrößert aber auch die Angriffsfläche (siehe ID 3.1.7). Die fehlende oder deaktivierte Option, sichere kryptographische Übertragungsprotokolle einzusetzen, erhöht weiterhin das Risiko, dass übertragene Daten von Dritten abgefangen werden (siehe ID 3.1.2).

Ein dritter wesentlicher Faktor ist eine oft fehlende Robustheit des Betriebssystems gegen die Ausbreitung der Schadsoftware über den Browser hinaus. Obwohl moderne Browser eigene Sicherheitsvorkehrungen mitbringen, erweist sich dieser Basisschutz viel zu oft als wirkungslos. In diesen Fällen könnten entsprechende Sicherheitsmechanismen der Betriebssysteme eine Weiterverbreitung auf und über den PC unterbinden; gleichwohl ist zu beobachten, dass jene längst zur Verfügung stehenden Sicherheitsmechanismen etwa aus Unkenntnis, aus Bequemlichkeit oder aus Gründen fehlender personeller Ressourcen im professionellen Umfeld nicht in ausreichendem Maße angewandt werden.

Zu bedenken ist, dass grundsätzlich Restrisiken verbleiben, selbst wenn der Web-Browser diesen Mindeststandard erfüllt. Die in diesem Mindeststandard definierten Sicherheitsanforderungen bieten somit keinen vollständigen Schutz gegen alle denkbaren Angriffsszenarien. Das bestehende Restrisiko bedeutet jedoch nicht, dass keinerlei Maßnahmen zu ergreifen sind. Entsprechend geeignete Maßnahmen sind als Ergebnis einer eigenen Risikoabschätzung auszuwählen. Eine (dokumentierte) Entscheidung die Risiken zu tragen ist dann möglich.

8 vgl. BSI (2016), S. 5ff.

4 Sicherheitsanforderungen

Nachfolgend werden Sicherheitsanforderungen an die Entwicklung (Kapitel 4.2) und den Betrieb (Kapitel 4.3) eines sicheren Web-Browsers aufgestellt. Für ein tieferes Verständnis wird zunächst (Kapitel 4.1) auf die wesentlichen Komponenten eines Web-Browsers eingegangen.

4.1 Aufbau Web-Browser (Komponenten)

Die Komponenten eines sicheren Web-Browsers und deren Zusammenhänge sind in Abbildung 1 dargestellt.

In diesem Aufbau übernimmt eine Managementkomponente, beispielsweise das Betriebssystem oder der Browser-eigene Ressourcenmanager, die Kontrolle über die ihm zugeordneten Unterprozesse wie Ausführungs- und Darstellungskomponenten oder Plug-ins. Eine Ausführungs- und Darstellungskomponente kann gleichzeitig in mehreren Tabs des Web-Browsers ausgeführt werden.

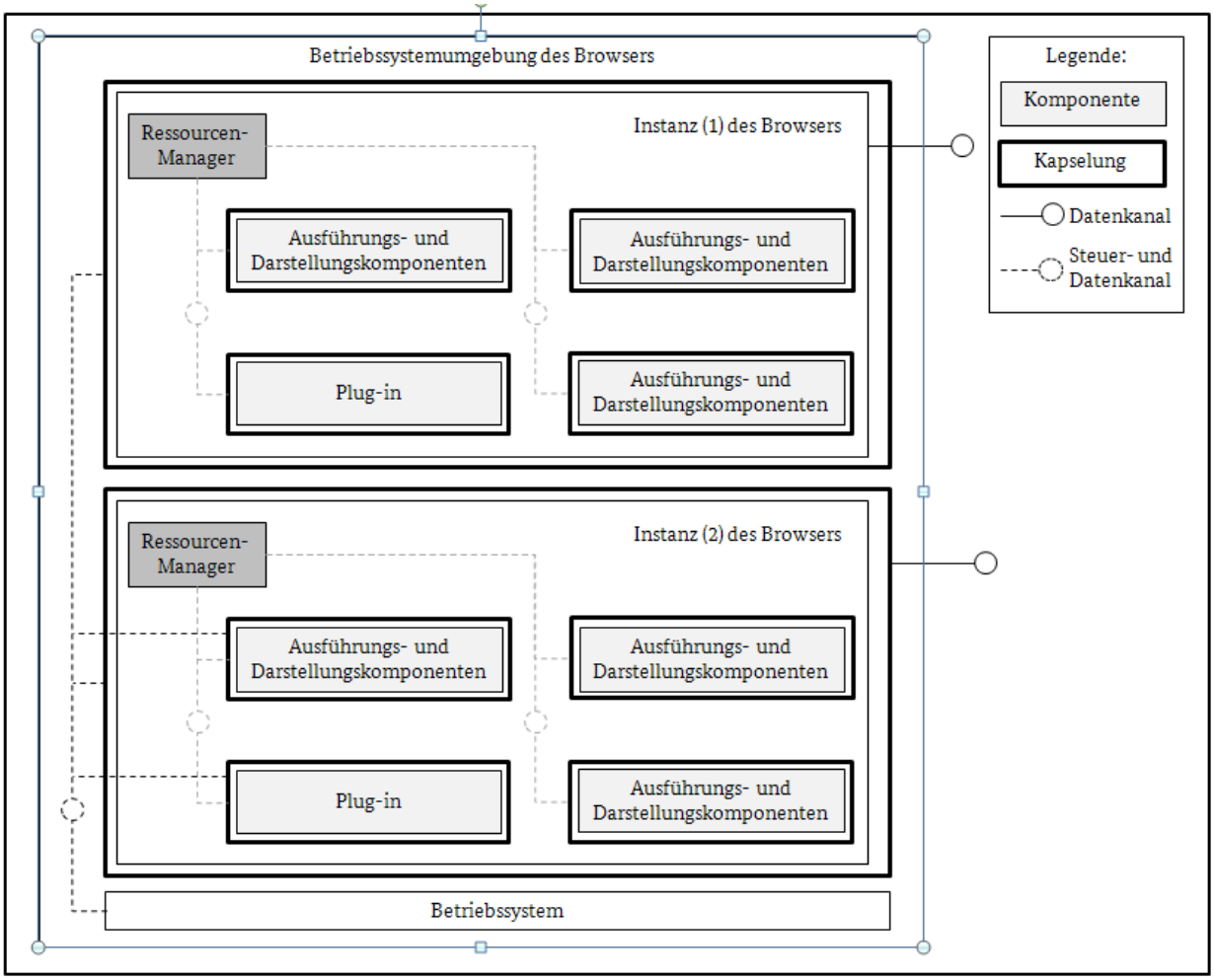

Abbildung 1: Schematische Darstellung Browser

Eine oder mehrere Komponenten sowie der Web-Browser selbst können derart gekapselt sein, dass jede Komponente im wesentlichen nur auf ihre eigenen Ressourcen, nicht aber auf andere zugreifen kann und umgekehrt (sog. Sandbox-Prinzip). Diese Kapselung wird auf mehreren Ebenen erreicht, beispielsweise auf Betriebssystemebene mittels Nutzer- und Berechtigungskonzept oder Filterung von Systemaufrufen. Auf Betriebssystemebene liegt der Web-Browser dann als Instanz bzw. eigener Prozess vor.

4.2 Sicherheitsanforderungen an Anbieter und Produkt

4.2.1 Funktionale Sicherheitsanforderungen

Kategorie	ID	Beschreibung
Vertrauenswürdige Kommunikation	4.2.1.1	Das Protokoll TLS in der Version 1.2 muss gem. Mindeststandard TLS 1.2 unterstützt werden.[9]
	4.2.1.2	– Der Web-Browser muss eine Liste von Zertifikaten vertrauenswürdiger Zertifikatsaussteller (CA-Zertifikat) bereitstellen. – Der Web-Browser muss Zertifikate mit erweiterter Prüfung (Extended-Validation-Zertifikate) unterstützen. – 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.
	4.2.1.3	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 (CRL oder OCSP).
	4.2.1.4	Der Web-Browser muss die Kommunikationsform geeignet und nicht manipulierbar darstellen: – Dem Benutzer muss beispielsweise durch Symbole oder farbliche Hervorhebung angezeigt werden, ob die Kommunikation mit dem Web-Server verschlüsselt oder im Klartext erfolgt. – Es muss die Möglichkeit bestehen, im Falle einer verschlüsselten Kommunikation auf Anforderung des Benutzers das verwendete Serverzertifikat, die verwendete SSL/TLS-Protokollversion und die Cipher-Suite anzeigen zulassen. – Dem Benutzer muss ein fehlendes CA-Zertifikat im Zertifikatsspeicher oder ein ungültiges/widerrufenes Serverzertifikat als Prüfergebnis signalisiert werden. Die verschlüsselte Verbindung darf dann nur nach expliziter Bestätigung durch den Benutzer aufgebaut werden.
	4.2.1.5	Der Web-Browser muss HSTS gem. RFC 6797[10] unterstützen.
Schutz des Webbrowsers	4.2.1.6	Software-Update-Mechanismen erfüllen folgende Anforderungen: – Software-Update-Mechanismen müssen sämtliche Web-Browser-komponenten umfassen (inkl. Erweiterungen und Plug-ins). Eigenständige Programme, die zusätzlich Elemente in den Browser einfügen (z. B. EXE-Dateien für Internet Explorer, die Buttons

9 vgl. BSI (2015), S. 6
10 vgl. RFC (2012)

Kategorie	ID	Beschreibung
		einrichten), müssen über separate Update-Prozesse aktuell gehalten oder untersagt werden. – Software-Updates müssen erkannt werden. – Software-Updates müssen zuverlässig angezeigt werden. – Automatisches Einspielen von Updates muss möglich sein.
	4.2.1.7	Integritätsprüfungen der Updates erfüllen folgende Anforderungen: – Updates dürfen nur dann eingespielt werden, wenn die Prüfung der Integrität ein positives Prüfergebnis liefert. – Nicht korrekte Prüfergebnisse müssen dem Benutzer signalisiert werden. Das Update darf in diesem Fall nicht eingespielt werden.
Identifikation und Authentisierung	4.2.1.8	Sichere Passwortmanager erfüllen folgende Eigenschaften: – Passwortmanager müssen eine eindeutige Zuordnung zwischen Webseite (URL) und hierfür gespeichertem Passwort zuverlässig ermöglichen. – Passwörter müssen besonders geschützt abgespeichert werden (z. B. verschlüsselt). Diese Sicherheitsanforderungen sind nur dann anzuwenden, wenn Passwortmanager genutzt werden. Zur Umsetzung können auch externe Add-ons verwendet werden.
	4.2.1.9	Der Passwortmanager darf einen Zugriff auf gespeicherte Passwörter nur nach Eingabe eines Master-Passworts durch den Benutzer ermöglichen. Jede neue Browser-Sitzung muss eine erneute Authentisierung für den Zugriff auf gespeicherte Passwörter erfordern.
	4.2.1.10	Bereits gespeicherte Passwörter und das Master-Passwort müssen auf Anforderung des Benutzers gelöscht werden können.
Schutz vertrauenswürdiger Daten	4.2.1.11	Das Anlegen von Cookies muss auf Anforderung des Benutzers deaktiviert werden können.
	4.2.1.12	Bereits angelegte Cookies müssen auf Anforderung des Benutzers gelöscht werden können.
	4.2.1.13	Die Nutzung von Drittanbieter-Cookies muss auf Anforderung des Benutzers blockiert werden können.
	4.2.1.14	Autofill-Funktionalitäten (Name, Email, usw.) müssen auf Anforderung des Benutzers deaktiviert werden können.
	4.2.1.15	Die Liste der besuchten Seiten (Historie) und die Autofill-Historien müssen auf Anforderung des Benutzers gelöscht werden können.
Überprüfung auf schädliche Inhalte	4.2.1.16	Adress- und inhaltsbasierte Schutzmechanismen (wie z. B. SafeBrowsing) sind implementiert.
	4.2.1.17	Adressbasierte Überprüfung: Liegen Informationen über schädliche Inhalte vor, muss der Benutzer beim Aufrufen der Webseite in

Kategorie	ID	Beschreibung
		geeigneter Form gewarnt werden. Die Überprüfung sollte vorrangig auf Basis lokal vorgehaltener Listen erfolgen. Eine als schädlich eingestufte Verbindung darf erst nach expliziter Bestätigung durch den Benutzer aufgebaut werden.
	4.2.1.18	Inhaltsbasierte Überprüfung: Vor eventuell schädlichem Inhalt (Dateien) wird der Benutzer entsprechend gewarnt.
Same-Origin-Policy	4.2.1.19	Eine sinnvolle Same-Origin-Policy ist umzusetzen. Insbesondere dürfen Dokumente und Skripte (Client) nicht auf Ressourcen (z. B. Grafiken, Textfelder) anderer Web-Seiten zugreifen.
	4.2.1.20	Herkunft (Origin) einer Webseite muss als Kombination aus den Parametern „Protokoll“, „Domain“ und ggf. angegebenem „Port“ in der Adresse (URL) ausgewertet werden. Ein Zugriff auf Ressourcen ist ausschließlich erlaubt, wenn alle drei Parameter in der URL identisch sind.
Sichere Konfiguration	4.2.1.21	Sichere Konfiguration: Eine zentrale Oberfläche für die Verwaltung der Einstellungen muss bereitstehen. Einstellungen, um Plug-ins, Erweiterungen und JavaScript aktivieren und deaktivieren zu können, müssen vorhanden sein.
	4.2.1.22	Zentrale Verwaltung: Der Import von zentral erstellten Konfigurationen muss möglich sein.
	4.2.1.23	Synchronisation: Sofern vorhanden, muss eine Synchronisation mit externen Speicherdiensten und -orten (sog. Cloud-Dienste) deaktivierbar sein.
	4.2.1.24	Browser-Instanzen: Der Web-Browser muss parallel in unterschiedlich konfigurierten Browser-Instanzen betrieben werden können.
Minimale Rechte	4.2.1.25	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 kann der Web-Browser mit erweiterten Rechten laufen, diese sind danach aber wieder abzutreten. – Lese- und Schreibzugriffe der Darstellungskomponenten sind ausschließlich auf festgelegte Bereiche des Dateisystems zulässig. – Aufrufe von Betriebssystemfunktionen durch Darstellungskomponenten dürfen ausschließlich über wohldefinierte Schnittstellen der Ressourcenmanager erfolgen.
Sandboxing und Kapselung	4.2.1.26	Der Web-Browser muss eine Architektur mit folgenden Eigenschaften bereitstellen: – Sämtliche Komponenten müssen voneinander und zum Betriebssystem hin gekapselt sein.

Kategorie	ID	Beschreibung
		– Direkter Zugriff auf Ressourcen isolierter Komponenten darf nicht möglich sein. – Kommunikation zwischen den isolierten Komponenten darf nur über definierte und kontrollierte Schnittstellen erfolgen. – Darstellungskomponenten für aktive Inhalte wie Flash und JavaScript sind gesondert gekapselt.
	4.2.1.27	Web-Seiten müssen voneinander isoliert werden, idealerweise in Form eigenständiger Prozesse. Eine Isolation auf Thread-Ebene ist aber ebenfalls zulässig.
	4.2.1.28	Der Web-Browser muss die Content Security Policy mindestens in der Version 1.0 gem. den W3C-Spezifikationen[11] umsetzen.

Tabelle 2: Funktionale Sicherheitsanforderungen an die Entwicklung

4.2.2 Organisatorische Sicherheitsanforderungen

Tabelle 3 stellt organisatorische Sicherheitsanforderungen dar, die Anbieter im Rahmen von Entwicklung und Wartung des Web-Browsers zu gewährleisten haben.

Kategorie	ID	Beschreibung
Entwicklung	4.2.2.1	Es sind nur Programmiersprachen und -werkzeuge zulässig, die sichere Funktionen unterstützen und Mechanismen zum Stack- und Heapschutz implementieren. Der Web-Browser muss die vom Betriebssystem bereitgestellten Speicherschutzmechanismen nutzen können.
Aktualisierung	4.2.2.2	Nach Bekanntwerden einer kritischen Schwachstelle soll durch den Anbieter innerhalb von 21 Tagen ein Software-Update zur Verfügung gestellt werden. Die Auslieferung der Updates muss integritätsgesichert erfolgen. (Für Anforderungen bzgl. Aktualisierungen an den Betreiber siehe ID 4.3.6.)
Fehlerbehebung	4.2.2.3	Um potenzielle Schwachstellen melden zu können, müssen Kontaktmöglichkeiten zu Sicherheitsteams des Anbieters bereitgestellt werden.
Datensicherheit	4.2.2.4	Um Überprüfungen auf schädliche Inhalte (u. a. Phishing) durchführen zu können, müssen aktuelle Listen bereitgestellt werden.

Tabelle 3: Organisatorische Sicherheitsanforderungen an die Entwicklung

11 vgl. W3C (2012)

4.3 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 in Tabelle 4 aufgeführten Sicherheitsanforderungen umzusetzen. Auf Kapitel 2.3 wird in diesem Zusammenhang hingewiesen.

Kategorie	ID	Beschreibung
Netzwerkumgebung	4.3.1	In der Netzwerkumgebung des Arbeitsplatzrechners sind folgende Maßnahmen umzusetzen: – Unverzügliches Einspielen sicherheitsrelevanter Patches und Updates (ausgenommen Browser-Patches, die in ID 4.2.2.2 und ID 4.3.6 separat behandelt werden). – Erkennung und Behandlung von Schadprogrammen. – Einsatz eines Paketfilters. – Maßnahmen für die Zugriffsrechte und -kontrolle.
Betriebssystem	4.3.2	Das Betriebssystem des Arbeitsplatzrechners muss dem Web-Browser Speicherschutzmechanismen wie ASLR, DEP oder eine sichere Ausnahmebehandlung bereitstellen.
Administration	4.3.3	Prozesse für folgende Maßnahmen sind vorzuhalten: – Pflege von Zertifikaten (siehe ID 4.2.1.2). – Unverzügliche Produktaktualisierung (siehe ID 4.2.1.6). – Verwaltung von Reputationslisten (siehe ID 4.2.1.18). – Verwaltung der Konfiguration (siehe ID 4.2.1.22).
Basiskonfiguration	4.3.4	Auslieferung in einer sicheren Basiskonfiguration: – Das Protokoll TLS, Version 1.2, muss gem. Mindeststandard TLS 1.2 aktiviert sein.[12] – Es muss geprüft werden, ob die Liste der Root-CAs eingeschränkt werden muss. – Für alle wichtigen öffentlichen TLS-verschlüsselten Web-Dienste sollten die Domains in die HSTS-Preload-Liste des Browsers eingefügt werden, um das Risiko einfacher Man-in-the-Middle-Angriffe zu verringern (siehe https://hstspreload.appspot.com). – Cookies von Drittanbietern werden nicht akzeptiert. – Die Ausführung von Plug-ins darf erst nach Bestätigung des Nutzers erfolgen (Click-to-Play). – EME[13] müssen deaktiviert werden, wenn diese nicht benötigt werden. – Die Autofill-Funktion ist deaktiviert. – Die integrierten Darstellungsmechanismen des Web-Browsers sind

12 vgl. BSI (2015), S.6
13 vgl. W3C (2016)

Kategorie	ID	Beschreibung
		aktiviert und werden bevorzugt verwendet. – Die Synchronisation von Daten (Cookies, Chronik, Lesezeichen, etc.) mit externen Speicherdiensten bzw. -orten (Cloud) ist deaktiviert. – Zentral vorgegebene Konfigurationen dürfen vom Benutzer nicht geändert werden.
Passwortqualität	4.3.5	Bei Nutzung eines Passwort-Managers sollte die Qualität des Logins vorgegeben werden.
Updates/Patches	4.3.6	Der Betreiber hat Updates nach ID 4.2.2.2 dieses Dokuments unverzüglich einzuspielen. Unabhängig von der Verfügbarkeit eines Updates nach Bekanntwerden einer kritischen Schwachstelle, muss der Betreiber nach spätestens 7 Tagen Maßnahmen zur Mitigation ergreifen. Dies könnte bspw. im Rahmen der vom BSI empfohlenen 2-Browser-Strategie[14] die zwischenzeitliche Abschaltung des betroffenen Browsers bedeuten.

Tabelle 4: Sicherheitsanforderungen an den Betrieb

14 Vgl. BSI (2013-2)

Literaturverzeichnis

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 (2013) Bundesamt für Sicherheit in der Informationstechnik: Sichere Inter-Netzwerk Architektur SINA, BSI-BRO13/322, 2013

BSI (2013-2) Bundesamt für Sicherheit in der Informationstechnik: Absicherungsmöglichkeiten beim Einsatz von Web-Browsern v1.0, 2013

BSI (2014) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, 14. Ergänzungslieferung, 2014

BSI (2015) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung, V1.0., 2015

BSI (2016) Bundesamt für Sicherheit in der Informationstechnik: Ransomware – Bedrohungslage, Prävention & Reaktion, Nationales IT-Lagezentrum, 2016

CVE The MITRE Corporation: „Common Vulnerabilities and Exposures, The Standard for Information Security Vulnerability Names“, http://cve.mitre.org; abgerufen am 22.03.2016

Mozilla (2015) Mozilla: Same-origin policy, https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy; abgerufen am 22.03.2016

RFC (2012) HTTP Strict Transport Security (HSTS), RFC 6797, IETF, 2012, https://tools.ietf.org/html/rfc6797

W3C (2012) Content Security Policy 1.0, W3C, 2012, https://www.w3.org/TR/2012/CR-CSP-20121115/

W3C (2016) Encrypted Media Extensions, W3C, 2016, https://www.w3.org/TR/2016/WD-encrypted-media-20160610/

Abkürzungsverzeichnis

ASLR	Address Space Layout Randomization
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DEP	Data Execution Prevention
EME	Encrypted Media Extensions
GG	Grundgesetz der Bundesrepublik Deutschland
IT	Informationstechnik
OCSP	Online Certificate Status Protocol
PDF	Portable Document Format
RFC	Request for Comments
SSL	Secure Sockets Layer
SINA	Sichere Inter-Netzwerk-Architektur
PDF	Portable Document Format
TLS	Transport Layer Security
URL	Uniform Resource Locator
W3C	World Wide Web Consortium

5 Anlagen

Hilfsdokument zum Mindeststandard Sichere Web-Browser

Tabellarischer Abgleich von Microsoft Internet Explorer und Edge, Mozilla Firefox und Google Chrome