Bundesamt
für Sicherheit in der
Informationstechnik

Erläuterungen zum Mindeststandard des BSI für sichere Web-Browser

Hinweise zu Interpretation und Umsetzung
Version 1.0

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

1 Über dieses Dokument

Das vorliegende Dokument unterstützt Sie bei Verständnis, Interpretation und Umsetzung des „Mindeststandards des BSI für sichere Web-Browser“. Hilfestellung bekommen Sie in vier Abschnitten:

Anwendung und Hintergrund

Hier erfahren Sie, was der Mindeststandard regelt, was er bewirken soll und wer ihn wie anzuwenden hat. Zudem finden Sie noch einige ganz knappe Grundlageninformationen über Mindeststandards, ihre gesetzliche Grundlage sowie ihre Bindungswirkung.

Interpretation einzelner Anforderungen

Die meisten Anforderungen im Mindeststandard werden für technisch versierte Leser klar verständlich sein, dennoch gibt es einige Punkte, die genauer erläutert werden sollten. Darunter fallen beispielsweise Anforderungen, die nicht scharf definiert sind (z. B. Virtualisierung) oder solche, die Browser nicht ohne Hilfe von Drittwerkzeugen erfüllen können (z. B. sicheres Passwort-Management).

Browser-Anpassungen

Eine andere Sichtweise liefert Ihnen dann eine kurze Übersicht, welche Maßnahmen Sie für welchen Browser durchführen müssen, um sie konform zum Mindeststandard zu betreiben.

Browser-Abgleich

Im Anhang finden Sie einen tabellarischen Abgleich der in der Bundesverwaltung gängigen Browser, also Mozilla Firefox, Google Chrome und Microsoft Internet Explorer und Edge.

Die Ausführungen in diesem Dokument sind lediglich als Hilfestellung gedacht und nicht rechtlich bindend. Ganz generell können Sie auslegbare Anforderungen anders als hier vorgeschlagen und gemäß der eigenen Bedürfnisse interpretieren und umsetzen – solange die Intention der Anforderung sowie der Wirkungsgrad unserer Interpretation berücksichtigt werden.

Ein Hinweis noch zur Aktualität: Die großen Browser werden kontinuierlich aktualisiert, verändert und gepatcht. Nicht alle Änderungen werden ohne Zeitverzögerung in diese Hilfe einfließen können. Und so werden sicherlich einzelne Punkte dieses Dokuments im Laufe der Zeit nicht mehr zu 100 Prozent zutreffen oder gar obsolet sein. Sollten Ihnen bei der Lektüre Unstimmigkeiten – nicht nur ob der Aktualität – auffallen, können Sie diese gerne an mindeststandards@bsi.bund.de berichten.

2 Anwendung

2.1 Was regelt der MST?

Der Mindeststandard für sichere Web-Browser adressiert Browser mit Zugriff auf das Internet. Er sorgt zum einen dafür, dass ausschließlich Browser eingesetzt werden, die ein Grundmaß an Sicherheit bieten. Zum anderen wird auf die Art und Weise eingegangen, wie ein solcher Browser eingesetzt wird.

Somit schützt der Standard vor allem vor bekannten Angriffsszenarien, typischen Einfallstoren wie veralteten Versionen, unsicheren Grundeinstellungen oder zu freizügigen Möglichkeiten für die Nutzer sowie unbedachtem (Fehl-) Verhalten. Hingegen schützt der Standard nicht wirkungsvoll gegen höherwertige Angriffe wie Advanced Persistent Threats (APTs) oder versierte Innentäter.

2.2 Wer soll den MST wann und wie anwenden?

Auch wenn Browser nicht traditionell über Ausschreibungen beschafft werden, muss dennoch an einem Punkt eine bewusste Entscheidung für ein Produkt getroffen werden. An dieser Stelle sind die Anforderungen des Mindeststandards zu berücksichtigen. Dabei muss der Browser nicht von Haus aus alle Anforderungen erfüllen – er muss es aber ermöglichen, diese Forderungen über organisatorische Maßnahmen oder Add-ons von Drittanbietern abzudecken.

Befindet sich ein Browser bereits im Betrieb, sind die Vorgaben aus dem Mindeststandard auch hier anzuwenden. In der Bundesverwaltung weit verbreitet sind Mozilla Firefox, Google Chrome und Microsoft Internet Explorer, die es allesamt ermöglichen, die aufgeführten Anforderungen – wenn auch teils über Umwege - zu erfüllen. In Hinblick auf Windows 10 wird auch Microsoft Edge betrachtet. Der Wechsel eines Browsers wird in den seltensten Fällen sein müssen, in der Regel. wird es genügen, Konfiguration und Betrieb gemäß Mindeststandard zu prüfen und gegebenenfalls anzupassen.

2.3 Ausnahmen

Der Standard sieht explizit keine Ausnahmen vor. In der Praxis wird es jedoch immer wieder begründete Einzelfälle geben, die exotische oder veraltete Browser bedingen, beispielsweise zum Betrieb etablierter Fachverfahren oder in eingebetteten Systemen. Sollten in solchen Fällen einzelne Anforderung nicht abgedeckt werden können, dokumentieren und begründen Sie die Entscheidung zu Ungunsten der IT-Sicherheit.

Sie sollten diese Ausnahmen schnellstmöglich durch standardkonforme Lösungen ablösen.

Auf der anderen Seite können natürlich auch exotische Browser alle Anforderung abdecken. Zum Beispiel bieten einige IT-Sicherheitsunternehmen gehärtete Versionen von Chrome und Firefox. Die Eignung konkreter Browser für konkrete Bedarfe muss die Behörde als Anwender selbst vornehmen, dieser Leitfaden beschränkt sich auf die vier wesentlichen und üblichen Produkte.

3 Auslegung und Umsetzung

Im Folgenden finden Sie Umsetzungshilfen und weitergehende Erläuterungen zu einigen komplexeren oder interpretierbaren Sicherheitsanforderungen aus Kapitel 4.2 des Mindeststandards für sichere Web-Browser. Sie bekommen hier Informationen darüber, welche der gängigen Browser (Firefox, Chrome, IE, Edge) welche Anforderungen von sich aus oder über zusätzliche Maßnahmen (z. B. Erweiterungen) erfüllen können.

Erfüllen mehrere Browser eine Anforderung, heißt dies natürlich nicht, dass sie sie gleich gut/genau umsetzen – tiefer gehende Analysen sollten Sie entsprechend der Bedürfnisse in Ihrer Organisation vornehmen.

Die Ausführungen gelten für die aufgeführten Browser in folgenden Versionen:

Mozilla Firefox 51.0.1
Google Chrome 56.0.2924.87
Microsoft Internet Explorer 11.103.14393.0
Microsoft Edge 38.14393.0.0

3.1 Anforderung 4.2.1.4: Kommunikationsform darstellen

Der Originaltext:

> 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 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.

Diese Anforderungen beziehen sich auf die Darstellung der Verbindungsdetails einer aufgerufenen URL. Typischerweise findet sich diese Funktion oben links neben dem Adressfeld der Browser, wo Details von TLS-Verbindungen mit Schloss-Symbolen und/oder farblichen Hinweisen in Ampel-Manier visualisiert werden. Über diese Schaltflächen lassen sich in der Regel weitere technische Informationen aufrufen. Werden bei der Verbindung Ungereimtheiten wie abgelaufene Zertifikate festgestellt, muss der Browser den Verbindungsaufbau stoppen, den Nutzer darauf hinweisen und explizit um Erlaubnis fragen, fortfahren zu dürfen.

Chrome, Internet Explorer und Firefox erfüllen diese Anforderungen standardmäßig. Microsoft Edge bietet bislang keine Möglichkeit, Zertifikate und Details anzuzeigen.

3.2 Anforderung 4.2.1.6: Update-Mechanismen

Der Originaltext:

> Software-Update-Mechanismen erfüllen folgende Anforderungen:

- Software-Update-Mechanismen müssen sämtliche Web-Browserkomponenten umfassen (inkl. Erweiterungen und Plug-ins). 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.
  - Software-Updates müssen erkannt werden.
  - Software-Updates müssen zuverlässig angezeigt werden.
  - Automatisches Einspielen von Updates muss möglich sein.

Der Browser muss Updates erkennen, anzeigen und automatisch einspielen – und zwar für alle Komponenten inklusive Add-ons.

Firefox und Chrome sind konform, Erweiterungen werden direkt über die Browser installiert, deinstalliert und über das Browser-Update aktualisiert..

Internet Explorer und Microsoft Edge erfüllen diese Anforderung mit leichten Mehraufwand: Erweiterungen für Edge werden über die eigenständige Anwendung Windows Store verwaltet. Erweiterungen für den Internet Explorer sind in der Regel komplett eigenständige Programme, die über die normalen Windows-Installationsroutinen, nicht über den Browser selbst, installiert und deinstalliert werden. Für derartige Software müssen eigene Maßnahmen zur Aktualisierung getroffen werden. Häufig werden für Anwendungsprogramme auf Arbeitsplatzrechnern bereits Sicherheitskonzepte bestehen.

Eine weitere mögliche Lösung wäre der gänzliche Verzicht auf Erweiterungen.

3.3 Anforderung 4.2.1.8: Passwortmanager

Der Originaltext:

> 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.

Alle Browser bieten standardmäßig das Speichern eingegebener Login-Daten an, allerdings bietet lediglich Firefox die Möglichkeit, diese gespeicherten Werte erst nach Eingabe eines Masterpassworts auslesen zu können. Und auch diese Option muss aktiviert werden.

Für Internet Explorer, Edge und Google Chrome gibt es zwei Optionen: Entweder, die Funktion zum Speichern von Passwörtern wird komplett deaktiviert oder es wird eine Lösung in Form von Drittanbieter-Werkzeugen genutzt. Entsprechende Programme gibt es auch als freie Lösungen unter Open-Source-Lizenzen. In den jeweiligen offiziellen Angeboten für Browser-Erweiterungen finden sich zahlreiche Lösungen, die mehr Sicherheit bieten als es die Browser standardmäßig tun.

3.4 Anforderung 4.2.1.22: Import zentraler erstellter Konfigurationen

Der Originaltext:

> Zentrale Verwaltung: Der Import von zentral erstellten Konfigurationen muss möglich sein.

Um Browser effizient einheitlich auszurollen und zu konfigurieren, müssen sie über vorgefertigte, zentral erstellte Konfigurationen eingerichtet werden können. Dies kann beispielsweise über den Import von expliziten Config-Dateien, Profile oder Gruppenrichtlinien erfolgen.

Chrome, Internet Explorer, Edge und Firefox können vorgefertigte Konfigurationen/Profile importieren bzw. übernehmen. Unter Windows ist ebenso eine Verwaltung über Gruppenrichtlinien möglich; Firefox benötigt dafür allerdings ein Add-on oder einen anderen Workaround.

3.5 Anforderung 4.2.1.24: Instanzen

Der Originaltext:

> Browser-Instanzen: Der Web-Browser muss parallel in unterschiedlich konfigurierten Browser-Instanzen betrieben werden können.

Um unterschiedlichen Sicherheitsbedürfnissen gerecht zu werden, muss ein Browser in mehreren, unterschiedlich konfigurierten Instanzen laufen können. So ließe sich der Browser etwa speziell für Fachverfahren mit erhöhter Sicherheit und parallel zum allgemeinen Surfen mit mehr Freiheiten einsetzen.

Firefox bietet diese Möglichkeit direkt. Chrome kann als portable Version in mehreren Instanzen parallel laufen. Internet Explorer und Edge sind nicht dafür ausgelegt. Lösungen könnten beispielsweise ein zweiter Browser oder Virtualisierung sein.

3.6 Anforderung 4.2.1.25: Minimale Rechte

Der Originaltext:

> 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.

Bestimmte Betriebssystemfunktionen werden für die Umsetzung eines Web-Browsers benötigt. Das Prinzip der minimalen Rechte wird dabei unterschiedlich umgesetzt. Unter Microsoft Windows haben die Ressourcenmanager von Internet Explorer, Edge, Chrome und Firefox mittlere Integrity Level. Die Darstellungskomponenten laufen anschließend mit niedrigeren Rechten. Die Browser sollten nicht mit dem Built-In-Administrator-Konto (das Standard-Admin-Konto, das bei der Installation eingerichtet wird) gestartet werden, denn dann wird der Ressourcenmanager ebenfalls mit hohem Integrity Level gestartet.

3.7 Anforderung 4.2.1.26: Architektur/Sandboxing

Der Originaltext:

> 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 und kontrollierte Schnittstellen erfolgen.
- Darstellungskomponenten für aktive Inhalte wie Flash und JavaScript sind gesondert gekapselt.

Die Anforderungen an die Architektur sollen sicherstellen, dass die angesprochenen Komponenten nicht in unerwünschter Weise auf andere Komponenten beziehungsweise deren Ressourcen zugreifen können. Alle vier betrachteten Browser werden dieser Anforderung gerecht, wenn auch in unterschiedlicher Ausprägung.

Ein simples Beispiel verdeutlicht das Prinzip des Sandboxing: Die Kapselung sorgt bei Firefox unter Mac OS X in der aktuellen Implementierung auf Content-Ebene dafür, dass Schreibzugriffe auf den größten Teil des Dateisystems sowie Schreib- und Lesezugriffe auf das Profil-Verzeichnis, soweit nicht benötigt, geblockt werden.

Die Implementierungen des Sandbox-Konzepts sind technisch wie qualitativ sehr unterschiedlich, jedoch erfüllen alle betrachteten Browser diese Anforderung.

3.8 Anforderung 4.2.1.27: Webseiten voneinander isoliert

Der Originaltext:

> Web-Seiten müssen voneinander isoliert werden, idealerweise in Form eigenständiger Prozesse. Eine Isolation auf Thread-Ebene ist aber ebenfalls zulässig.

Diese Anforderung zielt darauf ab zu verhindern, dass Webseiten auf die Ressourcen anderer geöffneter Webseiten zugreifen können. Die aktuellen Versionen der betrachteten Browser erfüllen dieses Kriterium. Jüngst hinzu gestoßen ist Firefox, der seit Version 48 multiprozessfähig ist. Sollte eine ältere Version des Mozilla-Browsers zum Einsatz kommen: Firefox vor Version 48 hat Tabs lediglich auf Thread- statt auf Prozessebene getrennt, was nach Interpretation des BSI immer noch genügend wäre.

4 Browser-Anpassungen

Als Ergänzung zur obigen ausführlichen Darstellung finden Sie folgend nochmal zusammengefasst die notwendigen Maßnahmen, um die einzelnen Browser konform zum Mindeststandard zu betreiben. Dabei wird lediglich auf solche Anforderungen verwiesen, die in diesem Dokument behandelt wurden und von den Browsern nicht standardmäßig erfüllt werden. Da es sich lediglich um eine Übersicht der wichtigsten Erkenntnisse/Maßnahmen aus Kapitel 3 handelt, wird auf weitergehende Erklärungen verzichtet.

4.1 Mozilla Firefox

– Master-Passwort muss aktiviert werden.

4.2 Google Chrome

– Passwort-Manager samt Master-Passwort muss per Add-on installiert werden; alternativ kann auf einen Passwort-Manager verzichtet werden.

4.3 Microsoft Internet Explorer

– Maßnahmen zur Aktualisierung von Erweiterungen beziehungsweise deren Sperrung.

– Passwort-Manager samt Master-Passwort muss per Add-on installiert werden; alternativ kann auf einen Passwort-Manager verzichtet werden.

– Es muss ein zweiter Browser zur Verfügung stehen beziehungsweise kurzfristig verfügbar gemacht werden können; alternativ könnte auch ein zweiter, virtualisierter Internet Explorer genutzt werden.

4.4 Edge

– Möglichkeit zur detaillierten Anzeige von Zertifikaten muss geschaffen werden.

– Maßnahmen zur Aktualisierung von Erweiterungen beziehungsweise deren Sperrung.

– Passwort-Manager samt Master-Passwort muss per Add-on eingebaut werden; alternativ kann auf einen Passwort-Manager verzichtet werden.

– Es muss ein zweiter Browser zur Verfügung stehen beziehungsweise kurzfristig verfügbar gemacht werden können. Alternativ kann eine zweite, virtualisierte Instanz von Edge genutzt werden. Diese ist jedoch aktuell noch nicht verfügbar, seitens Microsoft aber mit der Option „Windows Defender Application Guard“ angekündigt.

5 Anhang

Tabellarischer Abgleich von Firefox, Chrome, Internet Explorer und Edge in separater Datei.