Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Abgleichstabelle zum Mindeststandard des BSI für Webbrowser

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
2.1a	09.07.2020	Aktualisierung der Firefox-Version von 75 auf 78 (ESR)
3.0	19.02.2024	Major Release – Erweiterung um mobile Browser

Tabelle 1: Versionsgeschichte der Abgleichstabelle zum Mindeststandard für Webbrowser

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

Inhalt

1 Über dieses Dokument

Dieses Dokument unterstützt Verantwortliche bei der Einhaltung des Mindeststandards des BSI für Webbrowser in der Version 3.0. Hierfür werden in Kapitel 2 die technischen (Kapitel 2.1) und organisatorischen (Kapitel 2.2) Sicherheitsanforderungen mit den in der Bundesverwaltung am häufigsten eingesetzten Webbrowsern abgeglichen. Nicht betrachtet werden die Sicherheitsanforderungen an den Betrieb (Kapitel 2.3 des Mindeststandards), da diese nicht vom Webbrowser, sondern von der nutzenden Einrichtung einzuhalten sind.

Die Hilfestellungen in diesem Dokument sind nicht rechtlich bindend und schließen keine anderen Lösungen aus. Insbesondere ist zu beachten, dass der Mindeststandard ein Mindestsicherheitsniveau beschreibt, das nicht unterschritten werden sollte. Jede Institution sollte zusätzlich – nicht nur bei erhöhten Sicherheitsbedürfnissen – eigene Betrachtungen vornehmen.

Die Ergebnisse des Abgleichs werden (zusätzlich zur textuellen Beschreibung) farblich dargestellt. Dabei werden die Farben wie folgt verwendet:

Grün: Der Webbrowser erfüllt die Anforderung ohne zusätzliche Maßnahmen.

Gelb: Der Webbrowser erfüllt die Anforderung nur teilweise oder nur mithilfe weiterer Maßnahmen. Beispielhafte Lösungen werden an den entsprechenden Stellen vorgeschlagen.

Rot: Der Webbrowser erfüllt die Anforderung nicht.

Grau: Die Anforderung ist hier nicht relevant (bei mobilen Browsern, wenn bspw. Anforderungen über Eigenschaften des Betriebssystems umgesetzt werden)

Der Abgleich wurde auf Basis der nachfolgenden Webbrowser-Versionen durchgeführt:

- Mozilla Firefox 120
- Google Chrome 119
- Microsoft Edge 119
- Google Chrome für Android 119
- Mozilla Firefox für Android 120
- Apple Safari für iOS 16

Durch die kontinuierliche Aktualisierung und Veränderung von Webbrowsern können sich stets Änderungen bezüglich des Abgleichs ergeben. Dieses Dokument wird jährlich aktualisiert und bezieht sich ausschließlich auf die angegebenen Browser-Versionen. Zwischenzeitlich können neue Hinweise gerne per E-Mail über mindeststandards@bsi.bund.de eingereicht werden.

2 Abgleich Sicherheitsanforderungen

2.1 Technische Sicherheitsanforderungen an Anbietende und Produkt

WB.2.1.01 – Vertrauenswürdige Kommunikation

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
a) Transport Layer Security (TLS)	ja Nicht empfohlene Ciphers werden unterstützt, können aber per Konfigurationsdatei mit `security.ssl3.*` deaktiviert werden.	ja Nicht empfohlene Ciphers werden unterstützt, können aber per Kommandozeilenschalter `--cipher-suite-blacklist=` deaktiviert werden.	ja Nicht empfohlene Ciphers werden unterstützt, können aber per Gruppenrichtlinie `TLSCipherSuiteDenyList` deaktiviert werden.	ja Nicht empfohlene Ciphers werden unterstützt, können aber per Konfigurationsdatei mit `security.ssl3.*` deaktiviert werden.	ja Ciphers können nicht deaktiviert werden, dadurch ist es möglich, dass Verbindungen mit Webseiten zwar als verschlüsselt angezeigt werden, die Verschlüsselung aber unsichere Ciphers nutzt. Für dieses Risiko sollten Nutzende sensibilisiert werden und ggf. keine sensiblen Daten auf den Mobilgeräten verarbeitet werden.	ja Ciphers können nicht deaktiviert werden, dadurch ist es möglich, dass Verbindungen mit Webseiten zwar als verschlüsselt angezeigt werden, die Verschlüsselung aber unsichere Ciphers nutzt. Für dieses Risiko sollten Nutzende sensibilisiert werden und ggf. keine sensiblen Daten auf den Mobilgeräten verarbeitet werden.

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
b) Zertifikate	ja	Konfiguration erforderlich Nutzt (auch) den Zertifikatsspeicher des Betriebssystems Online-OCSP-/CRL-Prüfungen müssen per Gruppenrichtlinie oder Registry-Eintrag aktiviert werden.	Konfiguration erforderlich Nutzt den Zertifikatsspeicher des Betriebssystems Online-OCSP-/CRL-Prüfungen müssen per Gruppenrichtlinie oder Registry-Eintrag aktiviert werden.	Konfiguration erforderlich Kann den Zertifikatsspeicher des Betriebssystems nutzen (Funktion muss aktiviert werden) OCSP-Modus muss in der Konfigurations-datei mit `security.OCSP.enabled` aktiviert werden.	Konfiguration erforderlich Online-OCSP-/CRL-Prüfungen müssen per Enterprise-Policy `EnableOnlineRevokationChecks` aktiviert werden.	ja Nutzt den Zertifikatsspeicher des Betriebssystems Informationen über Zertifikats-widerrufe werden gesammelt und von Apple bereitgestellt. OCSP-Anfragen werden gestellt, wenn Widerrufs-informationen nicht vorliegen.
c) Darstellung der Kommunikationsform	ja	teilweise Die vollständige URL wird durch Kopieren und (an anderer Stelle) Einfügen sichtbar. Mixed-Content wird in der Adresszeile nicht geeignet dargestellt	teilweise Die vollständige URL wird durch Kopieren und (an anderer Stelle) Einfügen sichtbar. Mixed-Content wird in der Adresszeile nicht geeignet dargestellt	ja	teilweise Mixed-Content wird in der Adresszeile nicht geeignet dargestellt	ja

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
d) HTTP Strict Transport Security (HSTS)	ja	ja	ja	ja	ja	ja

WB.2.1.02 – Updates

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
a) Update-Mechanismen	ja	ja	ja	Wird in der Regel über die entsprechenden App-Stores oder ein MDM aktualisiert. Eigene Update-Mechanismen sind nicht verfügbar.	Wird in der Regel über die entsprechenden App-Stores oder ein MDM aktualisiert. Eigene Update-Mechanismen sind nicht verfügbar.	Erhält Updates als Bestandteil des festen iOS-Softwarepakets im Zuge von Betriebssystem-Updates.
b) Integritätsprüfungen der Updates	ja	ja	ja	Wird über Mechanismen des Betriebssystems aktualisiert.	Wird über Mechanismen des Betriebssystems aktualisiert.	Wird über Mechanismen des Betriebssystems aktualisiert.

WB.2.1.03 – Schutz vertrauenswürdiger Daten

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
a) Cookies	ja	ja	ja	ja	ja	ja

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
b) Website-Daten und Verlauf	ja	ja	ja	ja	ja	ja
c) Kamera, Mikrofon und Standort	ja	ja	ja	ja	ja	ja
d) Telemetriedaten	ja	ja	eingeschränkt Übertragung von Telemetriedaten lässt sich zentral nur in „höherwertigen“ Windows-Versionen (Enterprise, Education, Server) per Gruppen-richtlinie „Allow Telemetry“ bzw. „Allow diagnostic data“ zusammen mit der Windows-Telemetrie[1] deaktivieren.	ja	ja	ja Als Einstellung des Betriebssystems (nicht einzeln für Safari konfigurierbar)

[1] Vgl. https://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization (abgerufen am 18.12.2023).
Für weitere Informationen zur Telemetrie unter Windows siehe Projekt SiSyPHuS des BSI: https://www.bsi.bund.de/dok/11713470

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
e) Privater / Inkognito-Modus	ja	ja	ja	ja	ja	ja

WB.2.1.04 – Externe Dienste

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.1.04 – Externe Dienste	ja	ja	ja	ja	ja	ja

WB.2.1.05 – Same-Origin-Policy

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.1.05 – Same-Origin-Policy	ja	ja	ja	ja	ja	ja

WB.2.1.06 – Sichere Konfiguration

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
a) Verwaltung der Einstellungen	ja	ja	ja	eingeschränkt JavaScript lässt sich nur über Konfigurations-dateien oder Erweiterungen deaktivieren	ja	ja

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
b) Zentrale Konfiguration	ja	EME kann nicht zentral deaktiviert werden.	EME kann nicht zentral deaktiviert werden.	EME kann nicht zentral deaktiviert werden.	EME kann nicht zentral deaktiviert werden.	EME nicht deaktivierbar Der Hersteller gibt an, dass die Nutzung der digitalen Rechteverwaltung *FairPlay* durch den Safari-Browser besonders gesichert sei und damit die Möglichkeit zur Abschaltung der entsprechenden Schnittstelle entfallen könne. Die vom Hersteller zur Verfügung gestellten Informationen reichen für eine Bewertung durch das BSI nicht aus.
c) Schutz vor Änderungen	ja	ja	ja	ja	ja	ja
d) Cloud-Dienste	ja	ja	ja	ja	ja	ja
e) DoH / DoT	ja	ja	ja	ja	ja	ja

WB.2.1.07 – Minimale Rechte

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.1.07 – Minimale Rechte	ja	ja	ja	Durch App-Sandbox keine erweiterten Rechte im Sinne der Anforderung.	Durch App-Sandbox keine erweiterten Rechte im Sinne der Anforderung.	Durch App-Sandbox keine erweiterten Rechte im Sinne der Anforderung.

WB.2.1.08 – Sandboxing und Kapselung

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
a) Architektur-eigenschaften	ja	ja	ja	ja	ja	ja
b) Isolation von Webseiten	ja	ja	ja	ja	ja	ja

WB.2.1.09 – Content Security Policy (CSP)

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.1.09 – Content Security Policy (CSP)	ja	ja	ja	ja	ja	ja

WB.2.1.10 – Subresource Integrity

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.1.10 – Subresource Integrity	ja	ja	ja	ja	ja	ja

2.2 Organisatorische Sicherheitsanforderungen an Anbietende und Produkt

WB.2.2.01 – Entwicklung

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.2.01 – Entwicklung	ja	ja	ja	Teilweise kein Schutz gegen Stack-Smashing	Teilweise kein Schutz gegen Stack-Smashing	Eine Überprüfung der IPA-Datei von Safari ist nicht möglich, da es fester Bestandteil von iOS ist und nicht separat vorliegt.

WB.2.2.02 – Aktualisierung

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.2.02 – Aktualisierung	ja	ja	ja	ja	ja	ja

WB.2.2.03 – Kontaktmöglichkeit

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.2.03 – Kontaktmöglichkeit	ja	ja	ja	ja	ja	ja

WB.2.2.04 – Dokumentation

Sicherheitsanforderung	*Mozilla Firefox*	*Google Chrome*	*Microsoft Edge*	*Firefox für Android*	*Chrome für Android*	*Apple Safari für iOS*
WB.2.2.04 – Dokumentation	ja[2]	ja[3]	ja[4]	ja[2]	ja[3]	ja[5]

[2] Vgl. https://www.mozilla.org/de/privacy/firefox/ (abgerufen am 25.01.2024)
[3] Vgl. https://www.google.com/chrome/privacy/whitepaper.html (abgerufen am 25.01.2024)
[4] Vgl. https://learn.microsoft.com/en-us/microsoft-edge/privacy-whitepaper/ (abgerufen am 25.01.2024)
[5] Vgl. https://www.apple.com/de/privacy/ (abgerufen am 25.01.2024)