|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Web-Browser"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300046 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc82155416)

[Dokumentenhistorie 3](#_Toc82155417)

[Inhaltsverzeichnis 4](#_Toc82155418)

[Allgemeine Festlegungen 5](#_Toc82155419)

[Ziel / Zweck 5](#_Toc82155420)

[Geltungsbereich 5](#_Toc82155421)

[Zuständigkeiten 6](#_Toc82155422)

[Genehmigungs- und Änderungsverfahren 6](#_Toc82155423)

[Aufbau des Dokuments 6](#_Toc82155424)

[Sicherheitsrichtlinie „Web-Browser" 7](#_Toc82155425)

[Basismaßnahmen 7](#_Toc82155426)

[Verwendung von Sandboxing (APP.1.2.A1) 7](#_Toc82155427)

[Unterstützung sicherer Verschlüsselung der Kommunikation (APP.1.2.A2) 7](#_Toc82155428)

[Verwendung von vertrauenswürdigen Zertifikaten (APP.1.2.A3) 7](#_Toc82155429)

[Versionsprüfung und Aktualisierung des Web-Browsers (APP.1.2.A4) 8](#_Toc82155430)

[Standardmaßnahmen 8](#_Toc82155431)

[Verwendung einer zentralen Basiskonfiguration (APP.1.2.A5) 8](#_Toc82155432)

[Kennwortmanagement im Web-Browser (APP.1.2.A6) 8](#_Toc82155433)

[Datensparsamkeit in Web-Browsern (APP.1.2.A7) 9](#_Toc82155434)

[Verwendung von Plug-ins und Erweiterungen (APP.1.2.A8) 9](#_Toc82155435)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc82155436)

[Einsatz einer isolierten Web-Browser-Umgebung (APP.1.2.A9 - CI) 10](#_Toc82155437)

[Verwendung des privaten Modus (APP.1.2.A10 - C) 10](#_Toc82155438)

[Überprüfung auf schädliche Inhalte (APP.1.2.A11 - CIA) 10](#_Toc82155439)

[Zwei-Browser-Strategie (APP.1.2.A12 - CIA) 10](#_Toc82155440)

# Allgemeine Festlegungen

## Ziel / Zweck

Web-Browser sind Anwendungsprogramme, die (Hypertext-)Dokumente, Bilder, Video-, Audio- und andere Datenformate aus dem Internet oder internen Web-Anwendungen abrufen, verarbeiten, darstellen, ausgeben und auf lokalen IT-Systemen speichern können. Ein weiterer Einsatzzweck von Web-Browsern ist die Übertragung von zwischen zwei IT-Systemen, dies kann innerhalb der Infrastruktur der <Institution> oder auch in Richtung Internet erfolgen.

Workstations, Notebooks, Smartphones oder Tablets sind heute ohne Web-Browser nicht vorstellbar, weil sehr viele geschäftliche Anwendungen entsprechende Inhalte bereitstellen oder sogar als klassischen Anwendungsersatz fungieren. Gleichzeitig werden diese Inhalte immer vielfältiger. So kommen immer weniger Webseiten ohne eingebettete Videos, animierte Elemente und andere aktive Inhalte aus. Moderne Web-Browser decken zudem eine große Bandbreite an Zusatzfunktionen ab, indem sie Plug-ins und externe Bibliotheken einbinden. Hinzu kommen Erweiterungen für bestimmte Funktionen, Datenformate und Inhalte. Die Komplexität moderner Web-Browser bietet ein hohes Potenzial für gravierende konzeptionelle Fehler und programmtechnische Schwachstellen. Konzeptionelle Fehler und programmtechnische Schwachstellen erhöhen nicht nur die möglichen Gefahren für Angriffe, sondern auch Bedienungsfehler durch die Benutzer. Die Folgen für die Verfügbarkeit, die Vertraulichkeit und die Integrität von Daten der <Institution> sind erheblich. Inhalte aus dem Internet sollten aus diesem Grunde aus Sicht des Web-Browsers generell als nicht vertrauenswürdig angesehen werden.

Diese Sicherheitsrichtlinie benennt Sicherheitsanforderungen für Web-Browser, die auf Workstations und Notebooks sowie teilweise auch auf Tablets und Smartphones eingesetzt werden. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines APP.1.2 "Web-Browser" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Web-Browser“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Web-Browser"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Verwendung von Sandboxing (APP.1.2.A1)

Die freigegebenen und eingesetzten Web-Browser auf den Workstations, Notebooks, Smartphones and Tablets dürfen mittels Sandboxing nur auf die eigenen Ressourcen pro Instanz und pro Verarbeitungsprozess zugreifen. Webseiten sind durch den Web-Browser als eigenständige Prozesse oder mindestens als eigene Threads voneinander zu isolieren. Plug-ins und Erweiterungen müssen ebenfalls in isolierten Bereichen ausgeführt werden. Der Web-Browser sollte die aktuelle Version der Content Security Policy (CSP) gemäß den Spezifikationen des World Wide Web Consortium (W3C) umsetzen.

### Unterstützung sicherer Verschlüsselung der Kommunikation (APP.1.2.A2)

Die freigegebenen und eingesetzten Web-Browser müssen Transport Layer Security (TLS) in der Version 1.2 und 1.3 unterstützen. Die nicht mehr als sicher eingestuften Versionen 1.1 und 1.0 von TLS sind entweder durch geeignete Konfiguration-Policies oder durch den Browser-Hersteller selbst deaktiviert werden.

Die freigegebenen und eingesetzten Web-Browser müssen den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen. Für alle wichtigen öffentlichen TLS-verschlüsselten Web-Dienste sollten die Domains in die HSTS-Preload-Liste des Browsers eingefügt werden.

### Verwendung von vertrauenswürdigen Zertifikaten (APP.1.2.A3)

Die freigegebenen und eingesetzten Web-Browser müssen eine integrierte und aktuelle Liste vertrauenswürdiger öffentlicher Wurzelzertifikats-Aussteller den Benutzern (Mitarbeitenden) bereitstellen. Zur Verbesserung der Benutzbarkeit des Browsers und der Vermeidung von Bedienfehlern durch den Mitarbeitenden sind die von der <Institution> selbst bereitgestellten Zertifikate (Self-signed) mit in die Liste der vertrauenswürdigen Zertifikate aufzunehmen.

Die freigegebenen und eingesetzten Web-Browser müssen Extended-Validation-Zertifikate (EV-TLS-Zertifikat) unterstützen.

Ein Wurzelzertifikate darf nur mit den Rechten eines Administrators hinzugefügt, geändert oder gelöscht werden. Zertifikate müssen durch den freigegebenen und eingesetzten Web-Browser lokal auf dem Client widerrufen werden können.

Die freigegebenen und eingesetzten Web-Browser müssen die Gültigkeit der Server-Zertifikate mithilfe des öffentlichen Schlüssels und unter Berücksichtigung des Gültigkeitszeitraums vollständig prüfen. Auch der Sperrstatus (CRL oder OCSP) der Server-Zertifikate muss vom Web-Browser geprüft werden. Die Überprüfung des Server-Zertifikats sollte primär mittels OCSP erfolgen. Bei der Überprüfung des Server-Zertifikats ist die komplette Zertifikatskette einschließlich des Wurzelzertifikats zu verifizieren.

Die freigegebenen und eingesetzten Web-Browser müssen dem Benutzer gut sichtbar und eindeutig zeigen, ob die Übertragung der Daten zwischen der Webseite und dem Browser im Klartext oder verschlüsselt erfolgt.

Der Benutzer sollte bei Bedarf das aktuell verwendete Serverzertifikat für eine manuelle Überprüfung sich anzeigen lassen können.

Grundsätzlich muss der freigegebene und vom Benutzer verwendete Web-Browser automatisch signalisieren, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Die Verbindung darf in einem solchen Fall nur nach ausdrücklicher Bestätigung durch den Benutzer (Mitarbeitenden) hergestellt werden. Idealerweise wird die ausdrückliche Bestätigung durch den Mitarbeitenden mit einer entsprechend vorgeschalteten Webseite durch den Proxy der <Institution> unterstützt.

### Versionsprüfung und Aktualisierung des Web-Browsers (APP.1.2.A4)

Die freigegebenen und eingesetzten Web-Browser müssen den eigenen Versionsstand sowie den Versionsstand aller geladenen oder aktivierten Erweiterungen und Plug-ins zuverlässig erkennen und den Benutzern anzeigen können.

Bekannt gewordenen Sicherheitsprobleme der genutzten Plug-ins und Erweiterungen in Web-Browsern sind im Rahmen der etablierten Prozesse des Patch- und Änderungsmanagements unverzüglich zu beseitigen. Die freigegebenen und eingesetzten Web-Browser sollten Funktions- und Sicherheitsaktualisierungen automatisch einspielen können. Solange kein Aktualisierung für eine bekannt gewordene kritische Schwachstelle verfügbar ist, sind zeitnah alternative Maßnahmen zur Risikominderung zu ergreifen.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Verwendung einer zentralen Basiskonfiguration (APP.1.2.A5)

Die freigegebenen und eingesetzten Web-Browser sollten zentral über die von der <Institution> verantworteten Managementsysteme konfiguriert werden. Zentral vorgegebene Einstellungen dürfen nicht von den Mitarbeitenden verändert werden können. Der Web-Browser sollte nicht mit erweiterten Rechten (bspw. Systemrechten oder administrativen Rechten) ausgeführt werden.

### Kennwortmanagement im Web-Browser (APP.1.2.A6)

Sofern die freigegebenen Web-Browser einen integrierten Kennwortmanager besitzen, sollte der Kennwortmanager des Browsers den Benutzernamen und das Passwort für die aufgerufene Webseite in einer direkten und eindeutigen Beziehung abspeichern.

Der Zugriff auf die im Kennwortmanager gespeicherten Benutzernamen und zugehörigen Passwörter darf erst nach erfolgreicher Authentisierung möglich sein. Die Authentisierung sollte durch die Eingabe eines Master-Kennworts erfolgen und nur für nur für die aktuelle Sitzung gültig sein. Sofern der Kennwortmanager auch zur Erstellung von Passwörtern genutzt werden kann, sind die Mindestvorgaben der der <Institution> zu beachten.

Die im Kennwortmanager hinterlegten Passwörter müssen durch den Benutzer jederzeit selektiv gelöscht werden können.

Anstatt dem vom Web-Browser angebotenen Kennwortmanager sollten die Mitarbeitenden der <Institution> eine für die übergreifende Passwortverwaltung bereitgestellte Anwendung verwenden. Denn durch die Nutzung dieser Anwendung besteht die Möglichkeit Web-Browser übergreifend die Kennwörter zu Verwendungen.

### Datensparsamkeit in Web-Browsern (APP.1.2.A7)

Die Einstellungen des Web-Browsers sollten so gewählt werden, dass "Cookies von Drittanbietern" abgelehnt werden. Durch den Benutzer sollten gespeicherte Cookies jederzeit gelöscht werden können.

Die Funktion zur Autovervollständigung von Daten in Formularen sollte durch den Benutzer oder zentral deaktiviert werden. Sofern die Funktion dennoch den Benutzern zur Verfügung gestellt wird, sollte der Benutzer die Formulardaten löschen können. Ebenfalls sollte der Benutzer die Historiendaten des Web-Browsers löschen können. Die Synchronisation von Favoriten oder aktuellen Web-Browser-Sessions oder Passwörtern via Cloud-Dienste sollte im Einklang mit der Strategie zur Cloud-Nutzung angewandt werden.

Telemetriefunktionen sowie das automatische Senden von Absturzberichten an den Hersteller des Web-Browsers sollten deaktiviert werden.

Der Web-Browser sollte auf Peripheriegeräte wie Mikrofon oder Webcam nur nach dedizierter Freigabe durch den Benutzer zugreifen können. Die freigegebenen und eingesetzten Web-Browser sollten Einstellungsmöglichkeiten für WebRTC, HSTS und JavaScript anbieten.

### Verwendung von Plug-ins und Erweiterungen (APP.1.2.A8)

Es sollten nur unbedingt notwendige Plug-ins und Erweiterungen für den Web-Browser installiert werden. Die Plug-ins und Erweiterungen sollten ausschließlich aus vertrauenswürdigen Quellen bezogen werden. Plug-ins und Erweiterungen für den Web-Browser sollten nur mit Administrationsrechten installiert werden dürfen. Die Ausführung von Web-Browser Plug-ins sollte mindestens initial vom Benutzer bestätigt werden müssen. Der Web-Browser sollte die Möglichkeit bieten, Erweiterungen zu konfigurieren und abzuschalten.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Einsatz einer isolierten Web-Browser-Umgebung (APP.1.2.A9 - CI)

Bei sehr hohem Schutzbedarf der Workstation oder des Notebooks oder der mit dem Web-Browser erreichbaren Ziele, sollten Web-Browser eingesetzt werden, die in einer isolierten Umgebung laufen. Dies kann bspw. eine Remote-Controlled-Browser-System-Lösung (ReCoBS) oder eine Browser-in-The-Box (BitBox) oder auf einem dedizierten IT-Systemen sein.

### Verwendung des privaten Modus (APP.1.2.A10 - C)

Die Benutzer (Mitarbeitenden) sollten den Web-Browser bei erhöhten Anforderungen an die Vertraulichkeit im sogenannten privaten Modus verwenden. Hierdurch werden keine Informationen oder Inhalte dauerhaft auf der Workstation, Notebook, Smartphone oder Tablet des Mitarbeitenden gespeichert. Zusätzlich sollten die freigegebenen Web-Browser so konfiguriert werden, dass lokale Inhalte (Cache, Cookies) beim Beenden gelöscht werden.

### Überprüfung auf schädliche Inhalte (APP.1.2.A11 - CIA)

Aufgerufene Internetadressen sollten durch den Web-Browser oder besser durch die dedizierte Cyberrisk-Lösung der <Institution> auf potenziell schädliche Inhalte geprüft werden.

Der Web-Browser und die Cyberrisk-Lösung der <Institution> sollen den Benutzer warnen bzw. den Aufruf blockieren, wenn Informationen über schädliche Inhalte vorliegen. Das verwendete Verfahren zur Erkennung von Threats darf nicht gegen gesetzliche Vorgaben aus dem Datenschutz und internen Vorgaben der <Institution> verstoßen.

### Zwei-Browser-Strategie (APP.1.2.A12 - CIA)

Sofern für den Web-Browser öffentlich bekannte Sicherheitsproblemen ohne Workaround oder kein Sicherheitsupdate vorliegt, sollte ein alternativer sicherer Web-Browser eines anderen Herstellers verwendet werden, so dass die Mitarbeitenden eine Ausweichmöglichkeit haben. Bei der Wahl des alternativen Web-Browser muss darauf geachtet werden, dass die genutzte Browser-Basis nicht identisch mit dem bisherigen Browser ist (siehe <https://de.wikipedia.org/wiki/Liste_von_Webbrowsern>).