APP.1: Client-Anwendungen

APP.1.2: Webbrowser

1 Beschreibung

1.1 Einleitung

Webbrowser sind Anwendungsprogramme, die (Hypertext-) Dokumente, Bilder, Video-, Audio- und andere Datenformate aus dem Internet abrufen, verarbeiten, darstellen, ausgeben und auf lokalen IT-Systemen speichern können. Ebenso können Webbrowser auch Daten ins Internet übertragen.

Stationäre und mobile Clients sind heute ohne Webbrowser nicht vorstellbar, weil sehr viele private und geschäftliche Anwendungen entsprechende Inhalte nutzen. Gleichzeitig werden diese Inhalte im Internet immer vielfältiger. Die meisten Webseiten nutzen eingebettete Videos, animierte Elemente und andere aktive Inhalte. Moderne Webbrowser 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 Webbrowser bietet ein hohes Potenzial für gravierende konzeptionelle Fehler und programmtechnische Schwachstellen. Sie erhöht nicht nur die möglichen Gefahren für Angriffe aus dem Internet, sondern birgt zusätzliche Risiken durch Programmier- und Bedienungsfehler.

Die Risiken für die Vertraulichkeit und Integrität von Daten sind erheblich. Ebenso ist die Verfügbarkeit des gesamten IT-Systems durch solche Schwachstellen bedroht. Internetinhalte müssen demzufolge aus Sicht des Webbrowsers grundsätzlich als nicht vertrauenswürdig angesehen werden.

1.2 Zielsetzung

Dieser Baustein beschreibt Sicherheitsanforderungen für Webbrowser, die auf Clients, also auf stationären und mobilen IT-Systemen sowie auch auf Tablets und Smartphones, eingesetzt werden.

1.3 Abgrenzung und Modellierung

Der Baustein APP.1.2 *Webbrowser* ist auf jeden Webbrowser anzuwenden.

Er enthält grundsätzliche Sicherheitsanforderungen, die bei der Installation und dem Betrieb von Webbrowsern für den Zugriff auf Daten aus dem Internet zu beachten und zu erfüllen sind.

Webbrowser sind eine der am häufigsten genutzten Anwendungen. Sie greifen auf ungeprüfte, potentiell schädliche Daten im Internet zu und stellen damit ein Einfallstor für Angreifer dar, um sich weiter auf das Betriebssystem auszubreiten. Um die Betriebssysteme abzusichern, sollten daher die Anforderungen der Bausteine der Schichten SYS.2 *Desktop-Systeme* und SYS.3.2 *Tablet und Smartphone* erfüllt werden.

Mit Browsern genutzte Webanwendungen sowie zuständige Server werden in den Bausteinen APP.3.1

Webanwendungen und APP.3.2 *Webserver* behandelt.

Allgemeine Anforderungen an den sicheren Einsatz von Software sind in diesem Baustein nicht enthalten. Sie sind im Baustein APP.6 *Allgemeine Software* zu finden, der zusätzlich zu diesem Baustein anzuwenden ist.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.1.2 *Webbrowser* von besonderer Bedeutung.

2.1 Ausführung von Schadcode durch Webbrowser

Webbrowser laden regelmäßig Daten aus nicht vertrauenswürdigen Quellen. Solche Daten können ausführbaren Schadcode enthalten, der Schwachstellen ausnutzen kann und das IT-System des Benutzers ohne dessen Kenntnis infiziert.

Dabei kann es sich um Code handeln, der durch den Webbrowser direkt ausgeführt werden kann, wie etwa JavaScript oder WebAssembly. Ebenso kann es auch ausführbarer Code eines Plug-ins oder einer Erweiterung im Kontext des Browsers sein, wie etwa Java oder Bestandteile von PDF-Dokumenten. Schließlich kann es sich auch um Code handeln, der vom Webbrowser auf den Client geladen und dort außerhalb des Browser-Prozesses ausgeführt wird. Werden die grundlegenden Schutzmechanismen moderner Webbrowser nicht ausreichend angewendet, werden die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Diensten des Clients oder möglicherweise sogar der mit ihm verbundenen Netze bedroht.

2.2 Exploit Kits

Schwachstellenlisten und sogenannte Exploit Kits erleichtern die Entwicklung individueller Schadsoftware erheblich. Cyberangriffe können automatisiert werden, um Drive-by-Downloads oder andere Verbreitungswege leicht und ohne Expertenwissen zu nutzen. Angreifer können ihnen bekannte Schwachstellen der Webbrowser, der verbundenen Ressourcen oder Erweiterungen ausnutzen, um Folgeangriffe vorzubereiten oder Code mit Schadfunktion auf den Clients zu laden und zu installieren. Oft wird durch den so auf den Clients geladenen Schadcode weitere Schadsoftware nachgeladen, die dann auf den Clients mit den Rechten der Benutzer ausgeführt wird.

2.3 Mitlesen der Internetkommunikation

Die grundlegende Sicherheit der Kommunikation im Internet hängt wesentlich vom eingesetzten Authentisierungsverfahren und von der Verschlüsselung der Daten auf dem Transportweg ab.

Fehlerhafte Implementierungen der entsprechenden Verfahren sind möglich und verhindern eine wirkungsvolle Authentisierung und Verschlüsselung. Viele Webdienste bieten außerdem immer noch veraltete Verschlüsselungsverfahren an. Somit kann ein Angreifer die Authentisierung von Servern unterlaufen oder die Kommunikation bzw. die Daten werden nicht wirkungsvoll verschlüsselt. Hierdurch können Informationen auf dem Übertragungsweg mitgelesen oder verändert werden. In der Vergangenheit wurden außerdem Zertifizierungsstellen kompromittiert. Angreifer konnten so an Zertifikate für fremde Websites gelangen.

2.4 Integritätsverlust in Webbrowsern

Werden Webbrowser, Plug-ins oder Erweiterungen aus nicht vertrauenswürdigen Quellen bezogen, können unabsichtlich und unbemerkt Schadfunktionen ausgeführt werden. Angreifer können beispielsweise Browserkomponenten wie Toolbars fälschen, um die Benutzer auf manipulierte Kopien von Webseiten zu locken, mit deren Hilfe Phishing-Angriffe durchgeführt werden. Bösartige Erweiterungen können Inhalte der betrachteten Webseiten manipulieren oder Daten ausspionieren und an den Angreifer senden.

2.5 Verlust der Privatsphäre

Werden Webbrowser unsicher konfiguriert, können vertrauenswürdige Daten zufällig oder böswillig unbefugten Dritten zugänglich gemacht werden. Auch Passwörter können ungewollt weitergegeben werden. Werden Cookies, Passwörter, Historien, Eingabedaten und Suchanfragen gespeichert oder unnötige Erweiterungen aktiviert, können Daten von Dritten oder von Schadprogrammen leichter missbräuchlich ausgelesen werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.2 *Webbrowser* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.1.2 *Webbrowser* vorrangig erfüllt werden:

APP.1.2.A1 Verwendung von grundlegenden Sicherheitsmechanismen (B)

Der eingesetzte Webbrowser MUSS sicherstellen, dass jede Instanz und jeder Verarbeitungsprozess nur auf die eigenen Ressourcen zugreifen kann (Sandboxing). Webseiten MÜSSEN als eigenständige Prozesse oder mindestens als eigene Threads voneinander isolierten werden. Plug-ins und Erweiterungen MÜSSEN ebenfalls in isolierten Bereichen ausgeführt werden.

Der verwendete Webbrowser MUSS die Content Security Policy (CSP) umsetzen. Der aktuell höchste Level der CSP SOLLTE erfüllt werden.

Der Browser MUSS Maßnahmen zur Same-Origin-Policy und Subresource Integrity unterstützen.

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

Der Webbrowser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Verbindungen zu Webservern MÜSSEN mit TLS verschlüsselt werden, sofern dies vom Webserver unterstützt wird. Unsichere Versionen von TLS SOLLTEN deaktiviert werden. Der Webbrowser MUSS den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen und einsetzten.

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

Falls der Webbrowser eine eigene Liste von vertrauenswürdigen Wurzelzertifikaten bereitstellt, MUSS sichergestellt werden, dass nur Administratoren diese ändern können. Falls dies nicht durch technische Maßnahmen möglich ist, MUSS den Benutzern verboten werden, diese Liste zu ändern. Außerdem MUSS sichergestellt werden, dass der Webbrowser Zertifikate lokal widerrufen kann.

Der Webbrowser MUSS die Gültigkeit der Server-Zertifikate mithilfe des öffentlichen Schlüssels und unter Berücksichtigung des Gültigkeitszeitraums vollständig prüfen. Auch der Sperrstatus der Server-Zertifikate MUSS vom Webbrowser geprüft werden. Die Zertifikatskette einschließlich des Wurzelzertifikats MUSS verifiziert werden.

Der Webbrowser MUSS dem Benutzer eindeutig und gut sichtbar darstellen, ob die Kommunikation im Klartext oder verschlüsselt erfolgt. Der Webbrowser SOLLTE dem Benutzer auf Anforderung das verwendete Serverzertifikat anzeigen können. Der Webbrowser MUSS dem Benutzer signalisieren, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Der Webbrowser MUSS in diesem Fall die Verbindung abbrechen, bis der Benutzer diese ausdrücklich bestätigt hat.

APP.1.2.A4 ENTFALLEN (B)
Diese Anforderung ist entfallen.

APP.1.2.A6 Kennwortmanagement im Webbrowser (B)
Wird ein Kennwortmanager im Webbrowser verwendet, MUSS er eine direkte und eindeutige Beziehung zwischen Webseite und hierfür gespeichertem Kennwort herstellen. Der Kennwortspeicher MUSS die Passwörter verschlüsselt speichern. Es MUSS sichergestellt werden, dass auf die im Kennwortmanager gespeicherten Passwörter nur nach Eingabe eines Master-Kennworts zugegriffen werden kann. Außerdem MUSS sichergestellt sein, dass die Authentisierung für den kennwortgeschützten Zugriff nur für die aktuelle Sitzung gültig ist.

Der IT-Betrieb MUSS sicherstellen, dass der verwendete Browser den Benutzern die Möglichkeit bietet, gespeicherte Passwörter zu löschen.

APP.1.2.A13 Nutzung von DNS-over-HTTPS (B)
Die Institution MUSS prüfen, ob die verwendeten Browser DNS-over-HTTPS (DoH) einsetzen. Es MUSS festgelegt werden, ob die Funktion verwendet werden soll.

Falls die Institution DNS-Server als Resolver verwendet, die über nicht vertrauenswürdige Netze angesprochen werden, SOLLTE DoH verwendet werden. Falls DoH verwendet wird, MUSS die Institution einen vertrauenswürdigen DoH-Server festlegen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.1.2 *Webbrowser*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.1.2.A5 ENTFALLEN (S)
Diese Anforderung ist entfallen.

APP.1.2.A7 Datensparsamkeit in Webbrowsern [Benutzer] (S)
Cookies von Drittanbietern SOLLTEN im Webbrowser abgelehnt werden. Gespeicherte Cookies SOLLTEN durch den Benutzer gelöscht werden können.

Die Funktion zur Autovervollständigung von Daten SOLLTE deaktiviert werden. Wird die Funktion dennoch genutzt, SOLLTE der Benutzer diese Daten löschen können. Der Benutzer SOLLTE außerdem die Historiendaten des Webbrowsers löschen können.

Sofern vorhanden, SOLLTE eine Synchronisation des Webbrowsers mit Cloud-Diensten deaktiviert werden. Telemetriefunktionen sowie das automatische Senden von Absturzberichten, URL-Eingaben und Sucheingaben an den Hersteller oder andere Externe SOLLTEN soweit wie möglich deaktiviert werden.

Peripheriegeräte wie Mikrofon oder Webcam sowie Standortfreigaben SOLLTEN nur für Webseiten aktiviert werden, bei denen sie unbedingt benötigt werden. Der Browser SOLLTE eine Möglichkeit bieten, WebRTC, HSTS und JavaScript zu konfigurieren bzw. abzuschalten.

APP.1.2.A8 ENTFALLEN (S)
Diese Anforderung ist entfallen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.1.2 *Webbrowser* exemplarische Vorschläge für Anforderungen

aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.1.2.A9 Einsatz einer isolierten Webbrowser-Umgebung (H)

Bei erhöhtem Schutzbedarf SOLLTEN Webbrowser eingesetzt werden, die in einer isolierten Umgebung, wie z. B. ReCoBS, oder auf dedizierten IT-Systemen ausgeführt werden.

APP.1.2.A10 Verwendung des privaten Modus [Benutzer] (H)

Der Webbrowser SOLLTE bei erhöhten Anforderungen bezüglich der Vertraulichkeit im sogenannten privaten Modus ausgeführt werden, sodass keine Informationen oder Inhalte dauerhaft auf dem IT-System des Benutzers gespeichert werden. Der Browser SOLLTE so konfiguriert werden, dass lokale Inhalte beim Beenden gelöscht werden.

APP.1.2.A11 Überprüfung auf schädliche Inhalte (H)

Aufgerufene Internetadressen SOLLTEN durch den Webbrowser auf potenziell schädliche Inhalte geprüft werden. Der Webbrowser SOLLTE den Benutzer warnen, wenn Informationen über schädliche Inhalte vorliegen. Eine als schädlich klassifizierte Verbindung SOLLTE NICHT aufgerufen werden können. Das verwendete Verfahren zur Überprüfung DARF NICHT gegen Datenschutz- oder Geheimschutz-Vorgaben verstoßen.

APP.1.2.A12 Zwei-Browser-Strategie (H)

Für den Fall von ungelösten Sicherheitsproblemen mit dem verwendeten Webbrowser SOLLTE ein alternativer Browser mit einer anderen Plattform installiert sein, der dem Benutzer als Ausweichmöglichkeit dient.

4 Weiterführende Informationen

4.1 Wissenswertes

- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 047: „Absicherungsmöglichkeiten beim Einsatz von Webbrowsern“
- Mindeststandard des BSI für den Einsatz des SSL/ TLS-Protokoll durch Bundesbehörden nach § 8 Abs. 1 Satz 1 BSIG
- Mindeststandard des BSI für sichere Webbrowser nach § 8 Absatz 1 Satz 1 BSIG
- Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS): BSI-PP-0040

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.1.2 *Webbrowser* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme