Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: INTERNET-DIENSTLEISTER

Sicherer Einsatz von JavaScript

Verwendung aktiver Inhalte durch Anbieter von Webanwendungen

Bei der Gestaltung moderner Internet-Angebote greifen Entwickler von Webseiten heute regelmäßig auf aktive Inhalte zurück, die gegenüber statischem HTML insbesondere einen höheren Grad an dynamischer Interaktion mit dem Nutzer erlauben. Mittels aktueller Webtechniken, wie HTML5 und JavaScript, werden im Browser ausgeführte Anwendungen möglich, die zuvor nur mit lokal installierten Programmen umsetzbar waren.

Die hohe Attraktivität solcher Lösungen sowohl für Anbieter von Webseiten als auch deren Nutzer erfordert die Umsetzung von umfangreichen Maßnahmen auf Seiten der Anbieter zu deren technischer Absicherung, um bestehenden Risiken hinreichend zu begegnen. Bei Berücksichtigung dieser Empfehlungen ist unter definierten Rahmenbedingungen im Kontext eines normalen Schutzbedarfs der Einsatz von bestimmten aktiven Inhalten in sicherheitstechnisch geeigneten Browsern vertretbar.

1 Aktive Inhalte

Die Nutzung von aktiven Inhalten jedweder Art ist grundsätzlich durch den Dienstanbieter auf das fachlich Notwendige zu beschränken. Sofern aktive Inhalte zum Einsatz kommen, sollte der Dienstanbieter ausschließlich verbreitete Webtechniken, deren Unterstützung bereits in modernen Browsern in Verbindung mit geeigneten Sicherheitsmaßnahmen integriert ist, verwenden; dazu gehören etwa HTML5-Elemente sowie JavaScript. Andere aktive, über das Internet verteilte und dann im Browser ausgeführte Techniken sollten aus sicherheitstechnischen Gründen grundsätzlich *nicht* verwendet werden. So wird eine mit diesen Techniken verbundene mangelnde Interoperabilität vermieden und die Angriffsfläche des Browsers wirksam minimiert.

Ein Dienstanbieter sollte bei der Verwendung von HTML5 und JavaScript beachten, dass die Ausführung von aktiven Inhalten durch Filter an Sicherheitsgateways oder Netzübergängen sowie durch den Nutzer selbst ggf. blockiert wird. Daher ist stets die Bereitstellung der über die Webseite angebotenen Dienste und Dienstleistungen auch ohne die Verwendung aktiver Inhalte auf Seiten des Nutzers zu ermöglichen. Aktive Inhalte sollen die Nutzung der Webanwendung vereinfachen oder effizienter gestalten, jedoch keine zwingende Voraussetzung für die grundsätzliche Nutzung des Angebots bilden. Dies gilt insbesondere auch zur Gewährleistung einer barrierefreien Nutzung der Webseite.

Aufgrund der hier beschriebenen Eingrenzung auf wenige sicherheitstechnisch akzeptable aktive Inhalte, beschränken sich im Folgenden auch die empfohlenen Maßnahmen auf die Verwendung von JavaScript und HTML5. Obwohl die beschriebenen Maßnahmen auch bei anderen aktiven Inhalten ggf. eine Schutzwirkung entfalten können, stellen sie keine ausreichende Grundlage zu deren Absicherung dar. JavaScript im Kontext dieser Empfehlungen bezieht sich auf die ECMAScript® Language Specification[1] sowie die JavaScript Reference von Mozilla[2], HTML5 auf die entsprechenden Spezifikationen des World Wide Web Consortiums (W3C)[3].

2 Risiken

2.1 Risiken für Nutzer

Für den Nutzer einer Webseite mit aktiven Inhalten bestehen folgende wesentliche IT-Sicherheits-Risiken:

- Erhöhung der Angriffsfläche bei vorhandenen Schwachstellen im Browser durch erweiterte Möglichkeiten der Speicherkontrolle für den Angreifer mit dem Ziel des Ausbruchs aus der schützenden Sandbox des Browsers,
- Verletzung der Same-Origin-Policy des Browsers mit dem Ziel der Manipulation oder des Abhörens von Inhalten anderer Webseiten durch den Angreifer und
- eine unwissentliche Beteiligung des Nutzers an Distributed-Denial-of-Service-Angriffen (DDoS) mittels von Angreifern manipulierten und dann im Browser ausgeführten aktiven Inhalten, wie JavaScript-Code.

2.2 Risiken für Anbieter

Anbieter von Webseiten sind insbesondere gefährdet durch

- Man-in-the-Middle-Angriffe gegen den von ihnen ausgelieferten JavaScript-Code,
- Injektionsangriffe gegen die oder mittels der über aktive Inhalte ausgelieferten Funktionen und Schnittstellen zu Server-seitig gehaltenen Daten,
- Erhöhung der Angriffsfläche für Defacement-Angriffe mit gleichzeitig höherem Aufwand für die regelmäßigen Maßnahmen zu deren Erkennung,
- Erfordernis für im Vergleich zu statischen Inhalten umfangreicheren Tests vor einer öffentlichen Bereitstellung neuer Inhalte, verbunden mit dem Risiko unentdeckt bleibender Schwachstellen aufgrund der höheren Komplexität des Webangebots,
- die Client-seitige Verletzung der Same-Origin-Policy und damit Angriffe gegen die vom Anbieter bereitgestellten Inhalte bis hin zur Manipulation von auf dem Server gehaltenen Daten,
- Angriffe gegen die oder mittels der vom Anbieter verwendeten JavaScript-Bibliotheken, die dynamisch oder statisch in das eigene Angebot eingebunden werden und nicht vollständig unter Kontrolle des Anbieters stehen, und schließlich
- eine naturgemäß signifikant größere Bandbreite an Möglichkeiten, die Angreifern zur Kompromittierung von Client- und Serversystemen zur Verfügung steht und der damit mit differenzierten Maßnahmen wirksam begegnet werden muss.

1 http://ecma-international.org/ecma-262/5.1/
2 https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference
3 http://www.w3.org/TR/html5/

3 Erforderliche Voraussetzungen auf Seiten des Clients

Anbieter von Webangeboten mit aktiven Inhalten sind sicherheitstechnisch darauf angewiesen, dass die ihr Angebot nutzenden Clients verschiedene Voraussetzungen erfüllen, um eine Kompromittierung der Interaktion auf beiden Seiten zu vermeiden.

Ein sicherer Einsatz von JavaScript und HTML5 erfordert dabei den Einsatz von Browsern, die der BSI-Empfehlung für sichere Web-Browser[4] genügen. Dabei sind insbesondere die Anforderungen

> *1.3 (A) Ausführung des Web-Browsers mit minimalen Rechten, insbesondere für Darstellung des Inhalts*
>
> *1.4 (A) Weitestgehende Prozessisolation von voneinander getrennten Inhalten, einschließlich Plugins und gegenüber dem Betriebssystem (Sandboxing)*
>
> *2.1 (A) Möglichst fein-granulare Kontrolle der Ausführung von JavaScript, HTML5, WebGL und Flash sowie von installierten Erweiterungskomponenten und Plugins mit einfachen, sicheren Grundeinstellungen*
>
> *3.1 (A) Schnelle Bereitstellung von Aktualisierungen, insbesondere möglichst innerhalb von 24 Stunden, wenn die Schwachstelle bereits ausgenutzt wird*
>
> *3.2 (A) Schnelle und zuverlässige Verteilung von Aktualisierungen mittels automatischer Mechanismen, auch für Erweiterungskomponenten und Plugins*
>
> *5.2 (A) Möglichst weitgehende Umsetzung der Same-Origin-Policy*
>
> *6.8 (Z) Unterstützung von Mixed Content Blocking, wobei iFrames wie aktive Inhalte behandelt werden sollten*

von entscheidender Bedeutung.

Weitere von der Allianz für Cyber-Sicherheit veröffentlichte Absicherungsmöglichkeiten beim Einsatz von Web-Browsern[5] sind in der Lage, abhängig vom individuellen Schutzbedarf auf Clientseite eine sicherheitstechnisch hinreichende Ausführungsumgebung für einen Browser unter Nutzung aktiver Inhalte bereitzustellen. Zudem sind die Empfehlungen des IT-Grundschutz[6] und der ISi-Reihe des BSI[7], dort insbesondere zur sicheren Nutzung von Web-Angeboten (ISi-Web-Client)[8], zu beachten.

4 Server-seitige Maßnahmen

4.1 Abhängigkeiten zum verwendeten Browser

Anbieter von Webseiten müssen sicherstellen, dass das Angebot mit Browsern, die den in Kapitel 3 dargestellten Anforderungen genügen, vollständig dargestellt und genutzt werden kann. Browser- und Hersteller-spezifische Funktionen in HTML, JavaScript oder anderen Webtechniken sind daher zu vermeiden, insbesondere dann, wenn sie Nutzer zur Verwendung unsicherer Browser, Plugins oder anderer Komponenten zwingen. Es sollten ausschließlich Techniken, die auf offenen Standards[9] basieren, eingesetzt werden, um eine ausreichende Interoperabilität und sicherheitstechnische Überprüfbarkeit der Techniken zu ermöglichen.

Die Messung der aktuellen Verteilung der auf Nutzerseite eingesetzten Web-Browser ist – ab-

4 https://www.allianz-fuer-cybersicherheit.de/dok/6649780
5 https://www.allianz-fuer-cybersicherheit.de/dok/6649786
6 https://www.bsi.bund.de/grundschutz
7 https://www.bsi.bund.de/ISI-Reihe
8 https://www.bsi.bund.de/dok/6620620
9 https://ec.europa.eu/digital-agenda/en/open-standards

hängig von der konkreten Messmethode – mit systematischen Fehlern verbunden. Die Daten der Anbieter entsprechender Analysekomponenten oder Hosting-Infrastrukturen, wie z. B. StatCounter[10], W3Counter[11] oder Akamai[12], zeigen jedoch, dass heute der Einsatz von Web-Browsern, die in der Lage sind, dynamische Webangebote mit standardkonformen aktiven Inhalten zu verarbeiten, vorausgesetzt werden kann.

Insbesondere die automatischen Mechanismen zur Installation von Sicherheitsaktualisierungen in den am meisten verbreiteten Browsern zeigen hier Wirkung: Der Großteil der Nutzer setzt Browser in ihrer aktuellen Version ein, sodass die Umsetzung der erforderlichen Browser-seitigen Schutzmechanismen vom Anbieter der Webanwendung regelmäßig angenommen werden darf.

4.2 Absicherung des Webservers

Zur sicheren Bereitstellung von JavaScript auf Webservern ist die Umsetzung der umfangreichen Empfehlungen des Open Web Application Security Project (OWASP)[13] von zentraler Bedeutung. Dabei ist die Top-10-Liste der größten Sicherheitsrisiken Web-basierter Anwendungen[14] zu beachten, denen mit geeigneten Maßnahmen dauerhaft begegnet werden muss. Aktuell ist hierfür die Fassung von 2017[15] heranzuziehen.

Beim Einsatz von JavaScript sind insbesondere verschiedene Vorkehrungen zur Vermeidung von Cross-Site-Scripting (XSS)[16,17] und Cross-Site-Request-Forgery (CSRF)[18] zu treffen. Die Wirksamkeit der Maßnahmen sollte regelmäßig durch die probeweise Anwendung aktueller Angriffstechniken, wie sie z. B. im XSS Filter Evasion Cheat Sheet[19] beschrieben werden, im Rahmen von Penetrationstests getestet werden.

Mit der Verwendung von asynchronem JavaScript (Asynchronous JavaScript and XML, AJAX)[20] sind weitere Risiken verbunden, denen ebenfalls mit spezifischen Maßnahmen begegnet werden muss. Präventive Maßnahmen für die Client- und Server-seitige Absicherung von AJAX-Code liefern hierbei die AJAX Security Guidelines[21] des OWASP.

Weitere BSI-Empfehlungen für die Bereitstellung von Diensten im Internet bzw. Web-Angeboten geben der IT-Grundschutz sowie die ISi-Reihe (ISi-Web-Server)[22]. Insbesondere sollte die regelmäßige und kurzfristige Installation von Sicherheitsaktualisierungen für sämtliche verwendeten Produkte, Techniken und Bibliotheken umgesetzt werden.

5 Bibliotheken

Bei der Einbindung externer JavaScript-Bibliotheken, wie z. B. jQuery[23], ist sicherzustellen, dass externe Scripte stets aus einer vertrauenswürdigen Quelle über eine sichere Verbindung geladen werden. Daher müssen solche Bibliotheken, wenn die Vertrauenswürdigkeit der Quelle nicht zweifelsfrei und dauerhaft garantiert werden kann, vollständig vom Anbieter bezogen, abhängig vom individuellen Schutzbedarf der eigenen Web-Anwendung hinreichend auditiert und anschließend auf dem unter eigener Kontrolle stehenden Web-Server selbst gehostet wer-

10 http://gs.statcounter.com/
11 http://www.w3counter.com/globalstats.php
12 http://www.akamai.com/html/io/io_dataset.html
13 https://www.owasp.org/index.php/About_OWASP
14 https://www.owasp.org/index.php/OWASP_Top_10
15 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
16 https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet
17 https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet
18 https://www.owasp.org/index.php/CSRF_Prevention_Cheat_Sheet
19 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
20 https://developer.mozilla.org/de/docs/Web/Guide/AJAX
21 https://www.owasp.org/index.php/OWASP_AJAX_Security_Guidelines
22 sshttps://www.bsi.bund.de/ISi-Reihe
23 https://jquery.com/

den. Die Verfügbarkeit der Bibliotheken unter einer freien Lizenz[24] versetzt den Anbieter prinzipiell in die Lage, diese Anforderungen geeignet umzusetzen. Bei Lösungen unter anderen Lizenzen müssen ggf. vorab gesonderte Vereinbarungen mit dem jeweiligen Hersteller getroffen werden. Die Einbindung über eine wie oben beschriebene gesicherte Verbindung soll den Anforderungen der Technischen Richtlinie BSI TR-02102-2 „Verwendung von Transport Layer Security (TLS)"[25] genügen.

Treten in Bibliotheken von externen Anbietern Schwachstellen auf, sind kurzfristig Maßnahmen zu deren Eindämmung (Mitigation) zu ergreifen, bis eine Sicherheitsaktualisierung zur Verfügung steht. Sicherheitsaktualisierungen sind umgehend auf ihre Kompatibilität mit der eigenen Web-Anwendung zu testen und dann zu übernehmen. Die Aktualiserung der Bibliotheken ist immer dann selbst sicherzustellen, wenn mit lokalen Instanzen der Bibliotheken auf dem eigenen Webserver gearbeitet wird.

6 Fazit

Unter den mit dieser BSI-Veröffentlichung beschriebenen Randbedingungen und bei Umsetzung der sicherheitstechnisch erforderlichen Maßnahmen ist eine Nutzung von aktiven Inhalten möglich. Für Clients und Server mit einem normalen Schutzbedarf bleibt das Risiko beherrschbar. Dennoch ist der Einsatz aktiver Inhalte stets auf das fachlich Notwendige zu beschränken. Technisch dürfen nur verbreitete aktive Webtechniken, deren Unterstützung bereits in modernen Browsern in Verbindung mit geeigneten Sicherheitsmaßnahmen integriert ist, genutzt werden. Auf Grundlage der obigen Ausführungen wird geschlussfolgert, dass dies aktuell bei Einsatz von HTML5-Elementen und JavaScript der Fall ist.

Die Ausführung von aktiven Inhalten kann zur Sicherstellung der Barrierefreiheit und durch Filter an Sicherheitsgateways oder Netzübergängen sowie durch den Nutzer selbst blockiert werden. Daher sollte die Bereitstellung der über die Webseite angebotenen Dienste und Dienstleistungen immer auch ohne die Verwendung Client-seitig ausgeführter aktiver Inhalte erfolgen können.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

24 http://opensource.org/licenses
25 https://www.bsi.bund.de/dok/6623730