Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.1 Webanwendungen und Webservices

1. Beschreibung

1.1. Einleitung

Webanwendungen bieten bestimmte Funktionen und dynamische (sich verändernde) Inhalte. Dazu nutzen Webanwendungen die Internetprotokolle HTTP (Hypertext Transfer Protocol) oder HTTPS. Bei HTTPS wird die Verbindung durch das Protokoll TLS (Transport Layer Security) kryptografisch abgesichert. Webanwendungen stellen auf einem Server Dokumente und Bedienoberflächen, z. B. in Form von Eingabemasken, bereit und liefern diese auf Anfrage an entsprechende Programme auf den Clients aus, wie z. B. an Webbrowser.

Webservices sind Anwendungen, die das HTTP(S)-Protokoll verwenden, um Daten für andere Anwendungen bereitzustellen. In der Regel werden sie nicht unmittelbar durch Benutzende angesteuert.

Um eine Webanwendung oder einen Webservice zu betreiben, sind in der Regel mehrere Komponenten notwendig. Üblich sind Webserver, um Daten auszuliefern und Applikationsserver, um die eigentliche Anwendung oder den Webservice zu betreiben. Außerdem werden zusätzliche Hintergrundsysteme benötigt, die oft als Datenquellen über unterschiedliche Schnittstellen angebunden sind, z. B. Datenbanken oder Verzeichnisdienste.

Webanwendungen und Webservices werden sowohl in öffentlichen Datennetzen als auch in lokalen Netzen einer Institution (Intranet) eingesetzt, um Daten und Anwendungen bereitzustellen. In der Regel müssen sich Clients authentisieren, um auf eine Webanwendung oder einen Webservice zugreifen zu können.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Webanwendungen und Webservices sicher einzusetzen sowie Informationen zu schützen, die durch sie verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf jede Webanwendung und jeden Webservice anzuwenden, die im Informationsverbund eingesetzt werden.

Anforderungen an Webserver und an die redaktionelle Planung eines Webauftritts werden in diesem Baustein nicht behandelt. Sie sind im Baustein APP.3.2 *Webserver* zu finden. Die Entwicklung von Webanwendungen wird im Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.

Webservice-Schnittstellen werden oft via Representational State Transfer (REST) und Simple Object Access Protocol (SOAP) realisiert. In diesem Baustein werden nur REST-basierte Webservices betrachten. Der Fokus liegt dabei auf der Lebenszyklusphase „Betrieb“. Sicherheitsanforderungen, die sich beispielsweise aus der Planung und Konzeption sowie Aussonderung und Notfallvorsorge ergeben, werden in diesem Baustein nicht betrachtet, sondern müssen gesondert im Rahmen einer Risikoanalyse ermittelt werden.

Allgemeine Anforderungen an die Auswahl von Software werden im Baustein APP.6 *Allgemeine Software* betrachtet.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.1 *Webanwendungen und Webservices* von besonderer Bedeutung.

2.1. Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung oder dem Webservice unzureichend protokolliert werden, können diese unter Umständen zu einem späteren Zeitpunkt nur schwer nachvollzogen werden. Die Ursachen für ein Ereignis sind dann möglicherweise nicht mehr ermittelbar. So können z. B. kritische Fehler oder unerlaubte Änderungen in der Konfiguration der Webanwendung übersehen werden.

2.2. Offenlegung sicherheitsrelevanter Informationen bei Webanwendungen und Webservices

Webseiten und Daten, die von einer Webanwendung oder einem Webservice generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu Datenbanken oder Versionsständen von Frameworks. Diese Informationen können es bei Angriffen erleichtern, gezielt Webanwendungen oder Webservices anzugreifen.

2.3. Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn Funktionen einer Webanwendung oder eines Webservices automatisiert genutzt werden, können so zahlreiche Vorgänge in kurzer Zeit ausgeführt werden. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann so z. B. versucht werden, gültige Kombinationen von Konten und Passwörtern zu erraten (Brute-Force). Außerdem kann eine Liste mit gültigen Konten erzeugt werden (Enumeration), falls die Webanwendung oder der Webservice Informationen über vorhandene Konten zurück gibt. Darüber hinaus können wiederholte Aufrufe von ressourcenintensiven Funktionen wie z. B. komplexen Datenbankabfragen für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden.

2.4. Unzureichende Authentisierung

Oft sollen spezielle Funktionen einer Webanwendung oder eines Webservices nur bestimmten Gruppen vorbehalten bleiben. Die entsprechenden Personen erhalten dann z. B. Konten, die exklusiv mit den notwendigen Zugriffsrechten ausgestattet sind. Unter diesen Konten authentisieren sich die Benutzenden zu Beginn jeder Sitzung in der Webanwendung oder dem Webservice, z. B. mit Kontoname und Passwort. Wird diese Authentisierung nicht korrekt konfiguriert, kann sie möglicherweise umgangen werden. Außerdem kann eine Webanwendung oder ein Webservice so konfiguriert werden, dass Zugangsdaten auf dem Webserver unsicher gespeichert werden. Im Falle eines erfolgreichen Angriffs verfügen Angreifende dann über große Mengen von Zugangsdaten, die sie auch an anderen Stellen einsetzen könnten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.1 *Webanwendungen und Webservice* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Beschaffungsstelle

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.1.A1 Authentisierung (B)

Der IT-Betrieb MUSS Webanwendungen und Webservices so konfigurieren, dass sich Clients gegenüber der Webanwendung oder dem Webservice authentisieren müssen, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür MUSS eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess SOLLTE dokumentiert werden.

Der IT-Betrieb MUSS geeignete Grenzwerte für fehlgeschlagene Anmeldeversuche festlegen.

APP.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A4 Kontrolliertes Einbinden von Dateien und Inhalten (B)

Falls eine Webanwendung oder ein Webservice eine Upload-Funktion für Dateien anbietet, MUSS diese Funktion durch den IT-Betrieb so weit wie möglich eingeschränkt werden. Insbesondere MÜSSEN die erlaubte Dateigröße, erlaubte Dateitypen und erlaubte Speicherorte festgelegt werden. Es MUSS festgelegt werden, welche Clients die Funktion verwenden dürfen. Auch MÜSSEN Zugriffs- und

Ausführungsrechte restriktiv gesetzt werden. Zudem MUSS sichergestellt werden, dass Clients Dateien nur im vorgegebenen erlaubten Speicherort speichern können.

APP.3.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A7 Schutz vor unerlaubter automatisierter Nutzung (B)

Der IT-Betrieb MUSS sicherstellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei MUSS jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Clients auswirken. Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, MUSS dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.

APP.3.1.A14 Schutz vertraulicher Daten (B)

Der IT-Betrieb MUSS sicherstellen, dass Zugangsdaten zur Webanwendung oder zum Webservice serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden. Dazu MÜSSEN Salted Hash-Verfahren verwendet werden.

Die Dateien mit den Quelltexten der Webanwendung oder des Webservices MÜSSEN vor unerlaubten Abrufen geschützt werden.

APP.3.1.A16 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A19 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

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

APP.3.1.A8 Systemarchitektur (S) [Beschaffungsstelle]

Sicherheitsaspekte SOLLTEN bereits während der Planung von Webanwendungen und Webservices betrachtet werden. Auch SOLLTE darauf geachtet werden, dass die Architektur der Webanwendung oder des Webservice die Geschäftslogik der Institution exakt erfasst und korrekt umsetzt.

APP.3.1.A9 Beschaffung von Webanwendungen und Webservices (S)

Zusätzlich zu den allgemeinen Aspekten der Beschaffung von Software SOLLTE die Institution mindestens folgendes bei der Beschaffung von Webanwendungen und Webservices berücksichtigen:

- sichere Eingabevalidierung und Ausgabekodierung,
- sicheres Session-Management,
- sichere kryptografische Verfahren,
- sichere Authentisierungsverfahren,
- sichere Verfahren zum serverseitigen Speichern von Zugangsdaten,
- geeignetes Berechtigungsmanagement,

- ausreichende Protokollierungsmöglichkeiten,
- regelmäßige Sicherheitsupdates durch den Entwickelnden der Software,
- Schutzmechanismen vor verbreiteten Angriffen auf Webanwendungen und Webservices sowie
- Zugriff auf den Quelltext der Webanwendung oder des Webservices.

APP.3.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A11 Sichere Anbindung von Hintergrundsystemen (S)

Der Zugriff auf Hintergrundsysteme, auf denen Funktionen und Daten ausgelagert werden, SOLLTE ausschließlich über definierte Schnittstellen und von definierten IT-Systemen aus möglich sein. Bei der Kommunikation über Netz- und Standortgrenzen hinweg SOLLTE der Datenverkehr authentisiert und verschlüsselt werden.

APP.3.1.A12 Sichere Konfiguration (S)

Webanwendungen und Webservices SOLLTEN so konfiguriert sein, dass auf ihre Ressourcen und Funktionen ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade zugegriffen werden kann. Der Zugriff auf nicht benötigte Ressourcen und Funktionen SOLLTE deaktiviert werden. Falls dies nicht möglich ist, SOLLTE der Zugriff soweit wie möglich eingeschränkt werden. Folgendes SOLLTE bei der Konfiguration von Webanwendungen und Webservices umgesetzt werden:

- Deaktivieren nicht benötigter HTTP-Methoden,
- Konfigurieren der Zeichenkodierung,
- Vermeiden von sicherheitsrelevanten Informationen in Fehlermeldungen und Antworten,
- Speichern von Konfigurationsdateien außerhalb des Web-Root-Verzeichnisses sowie
- Festlegen von Grenzwerten für Zugriffsversuche.

APP.3.1.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.1.A21 Sichere HTTP-Konfiguration bei Webanwendungen (S)

Zum Schutz vor Clickjacking, Cross-Site-Scripting und anderen Angriffen SOLLTE der IT-Betrieb geeignete HTTP-Response-Header setzen. Dazu SOLLTEN mindestens die folgenden HTTP-Header verwendet werden:

- Content-Security-Policy,
- Strict-Transport-Security,
- Content-Type,
- X-Content-Type-Options sowie
- Cache-Control.

Die verwendeten HTTP-Header SOLLTEN so restriktiv wie möglich sein.

Cookies SOLLTEN grundsätzlich mit den Attributen *secure*, *SameSite* und *httponly* gesetzt werden.

APP.3.1.A22 Penetrationstest und Revision (S)

Webanwendungen und Webservices SOLLTEN regelmäßig auf Sicherheitsprobleme hin überprüft werden. Insbesondere SOLLTEN regelmäßig Revisionen durchgeführt werden. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert, ausreichend geschützt und vertraulich behandelt werden. Abweichungen SOLLTE nachgegangen werden. Die Ergebnisse SOLLTEN dem ISB vorgelegt werden.

APP.3.1.A23 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.1.A20 Einsatz von Web Application Firewalls (H)

Institutionen SOLLTEN Web Application Firewalls (WAF) einsetzen. Die Konfiguration der eingesetzten WAF SOLLTE auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices SOLLTE die Konfiguration der WAF geprüft werden.

APP.3.1.A24 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.3.1.A25 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Open Web Application Security Projekt (OWASP) stellt auf seiner Webseite Hinweise zur Absicherung von Webanwendungen und Webservices zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102“ Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.