APP.3: Netzbasierte Dienste

APP.3.1: Webanwendungen

1 Beschreibung

1.1 Einleitung

Webanwendungen bieten Anwendern 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 Benutzeroberflächen, z. B. in Form von Eingabemasken, bereit und liefern diese auf Anfrage an entsprechende Programme auf den Clients aus, wie z. B. an Webbrowser.

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

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

1.2 Zielsetzung

Ziel dieses Bausteins ist es, Webanwendungen sicher zu betreiben sowie Informationen zu schützen, die durch eine Webanwendung verarbeitet werden.

1.3 Abgrenzung und Modellierung

Der Baustein ist auf jede Webanwendung anzuwenden, die im Informationsverbund eingesetzt wird.

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.

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

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.3.1

Webanwendungen von besonderer Bedeutung.

2.1 Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung 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

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

2.3 Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn ein Angreifer Funktionen einer Webanwendung automatisiert nutzt, kann er zahlreiche Vorgänge in kurzer Zeit ausführen. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann der Angreifer z. B. versuchen, gültige Kombinationen von Benutzernamen und Passwörtern zu erraten (Brute-Force). Außerdem kann er Listen mit gültigen Benutzernamen erzeugen (Enumeration), falls die Webanwendung Informationen über vorhandene Benutzer 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 nur bestimmten Benutzergruppen vorbehalten bleiben. Die entsprechenden Benutzer erhalten dann z. B. Benutzerkonten, die exklusiv mit den notwendigen Zugriffsrechten ausgestattet sind. Unter diesen Benutzerkonten authentisieren sich die Benutzer zu Beginn jeder Sitzung in der Webanwendung, z. B. mit Benutzername und Passwort. Wird diese Authentisierung nicht korrekt konfiguriert, kann sie möglicherweise von einem Angreifer umgangen werden. Außerdem kann eine Webanwendung so konfiguriert werden, dass Zugangsdaten auf dem Webserver unsicher gespeichert werden. Im Falle eines erfolgreichen Angriffs verfügt der Angreifer dann über große Mengen von Zugangsdaten, die er auch an anderen Stellen einsetzen könnte.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.1 *Webanwendungen* 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	Beschaffungsstelle

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.3.1 *Webanwendungen* vorrangig erfüllt werden:

APP.3.1.A1 Authentisierung bei Webanwendungen (B)

Der IT-Betrieb MUSS Webanwendungen so konfigurieren, dass sich Benutzer gegenüber der Webanwendung 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 bei Webanwendungen (B)

Falls eine Webanwendung 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 Benutzer die Funktion verwenden dürfen. Auch MÜSSEN Zugriffs- und Ausführungsrechte restriktiv gesetzt werden. Zudem MUSS sichergestellt werden, dass ein Benutzer Dateien nur im vorgegebenen erlaubten Speicherort speichern kann.

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 von Webanwendungen (B)

Der IT-Betrieb MUSS sicherstellen, dass die Webanwendung vor unberechtigter automatisierter Nutzung geschützt wird. Dabei MUSS jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Benutzer 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 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 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 den Baustein APP.3.1 *Webanwendungen*. Sie SOLLTEN grundsätzlich erfüllt werden.

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

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

APP.3.1.A9 Beschaffung von Webanwendungen (S)

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

- sichere Eingabevalidierung und Ausgabekodierung in der Webanwendung,
- sicheres Session-Management,
- sichere kryptografische Verfahren,
- sichere Authentisierungsverfahren,
- sichere Verfahren zum serverseitigen Speichern von Zugangsdaten,
- geeignetes Berechtigungsmanagement innerhalb der Webanwendung,
- ausreichende Protokollierungsmöglichkeiten,
- regelmäßige Sicherheitsupdates durch den Entwickler der Software,
- Schutzmechanismen vor verbreiteten Angriffen auf Webanwendungen sowie
- Zugriff auf den Quelltext der Webanwendung.

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 von Webanwendungen (S)

Eine Webanwendung SOLLTE 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 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 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 den Baustein APP.3.1 *Webanwendungen* 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.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 angepasst werden. Nach jedem Update der Webanwendung 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 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.

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.3.1 *Webanwendungen* von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen