Goldene Regeln für den IT-Grundschutz-Baustein B 5.21 Webanwendungen

Webanwendungen stellen Funktionalitäten zur Verfügung, die über einen Web-Client (Browser) abrufbar ist. Benutzereingaben werden verarbeitet und die Resultate in dynamisch generierten Webseiten präsentiert. Häufig greift eine Webanwendung dabei auf unterschiedliche Hintergrundsysteme und -dienste (z. B. Datenbanken) zurück.

- Die Architektur der Webanwendung ist im Sicherheitskonzept zu dokumentieren. Anhand der Dokumentation muss nachvollziehbar sein, welche Komponenten existieren und welche Geschäfts- und Sicherheitsfunktionen implementiert sind.
- Bei Webanwendungen handelt es sich in der Regel um Individualsoftware oder um Anpassungen einer Standardsoftware (z. B. Content Management System). Als Basis für eine sichere Anwendung ist ein geregelter Entwicklungsprozess nach einem geeigneten Vorgehensmodell sicherzustellen. Dieses umfasst die Anforderungsanalyse, die Konzeption und das Design der Anwendung, die Entwicklung, das Testen sowie die Integration und die Softwareverteilung. Die Sicherheit der Webanwendung ist in allen Phasen zu berücksichtigen.
- Alle Daten aus nicht-vertrauenswürdigen Quellen, die von der Webanwendung verarbeitet werden, müssen in eine einheitliche Form überführt werden (z. B. durch Kanonalisierung) bevor sie validiert und ggf. enkodiert oder maskiert werden. Hier ist das Whitelist-Verfahren zu bevorzugen. Um Schwachstellen wie beispielsweise Cross-Site-Scripting (XSS) und SQL-Injection zu vermeiden, müssen für alle Daten entsprechende Validierungs- und ggf. Enkodierungs- und Filterfunktionen verwendet werden.
- Für den Zugriff auf sensitive Funktionen oder Informationen muss die Webanwendung eine wirksame Authentisierung und Sitzungsverwaltung unterstützen. Die Eigenschaften der Sitzungs-ID müssen so gewählt werden, dass die Sitzung ausreichend geschützt ist.
- Eine Zugriffskontrolle muss die unbefugte Nutzung geschützter Funktionen sowie die Einsicht und Manipulation von geschützten Informationen verhindern können.
- Die Webanwendung sollte schützenswerte Daten bei der Übermittlung sicher übertragen. Dazu sind unter anderem Direktiven in den HTTP-Headern (z. B. Caching- und Cookie-Felder) und der Einsatz verschlüsselter Verbindungen (z. B. SSL/TLS) zu berücksichtigen. Schützenswerte Daten dürfen nicht in der URL übertragen werden.
- Die Preisgabe interner Informationen (z. B. in Fehlermeldungen, HTTP-Headern) sollte möglichst restriktiv erfolgen. Nur Informationen, die für die Nutzung der Webanwendung notwendig sind, sollten dem Benutzer übermittelt werden.
- Fehler müssen so behandelt werden, dass sich die Webanwendung und die zugehörigen Komponenten zu jeder Zeit in einem sicheren Zustand befinden. Z. B. müssen Fehler bei der Autorisierung zu einer Verweigerung des Zugriffs führen.
- Die Logging-Funktionen der Webanwendung müssen alle sicherheitsrelevanten Ereignisse derart protokollieren, dass sicherheitskritische Vorfälle nachvollzogen werden können.
- Die Anwendungslogik sollte gegen automatisierte und logische Angriffe (z. B. DoS, Enumeration) geschützt werden. Dazu können Maßnahmen wie z. B. Grenzwerte für fehlgeschlagene Anmeldeversuche umgesetzt werden.
- Sicherheitsmechanismen (z. B. Authentisierung und Zugriffskontrolle) sind serverseitig zu implementieren und sollten durch clientseitige Mechanismen ergänzt werden, um Angriffe auf die Webanwendung über den Client abzuwehren.

Die Sicherheitsempfehlungen zum Thema Webanwendungen müssen zielgruppengerecht aufbereitet und institutionsweit veröffentlicht werden. Weitere Informationen zum Thema Webanwendungen finden sich im Baustein B 5.21 Webanwendungen und in den weiteren Bereichen der IT-Grundschutz-Kataloge.