



APP.3.2 Webserver

1. Beschreibung

1.1. Einleitung

Ein Webserver ist die Kernkomponente jedes Webangebotes, er nimmt Anfragen der Clients entgegen und liefert die entsprechenden Inhalte zurück. Die Daten werden in der Regel über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS) transportiert. Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Clients bieten, werden sie auch häufig für interne Informationen und Anwendungen in Institutionsnetzen, wie dem Intranet, eingesetzt.

Webserver sind in der Regel direkt im Internet verfügbar und bieten somit eine exponierte Angriffsfläche. Deswegen müssen sie durch geeignete Schutzmaßnahmen abgesichert werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz des Webserver und der Informationen, die durch den Webserver bereitgestellt oder damit verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein muss auf alle Webserver des Informationsverbunds angewendet werden.

Die Bezeichnung Webserver wird sowohl für die Software verwendet, welche die HTTP-Anfragen beantwortet, als auch für die IT-Systeme, auf denen diese Software ausgeführt wird. In diesem Baustein wird vorrangig die Webserver-Software betrachtet. Sicherheitsaspekte des IT-Systems, auf dem die Webserver-Software installiert ist, werden im Baustein SYS.1.1 *Allgemeiner Server* sowie den jeweiligen betriebssystemspezifischen Bausteinen betrachtet.

Empfehlungen, wie Webserver in die Netzarchitektur zu integrieren und mit Firewalls abzusichern sind, finden sich in den Bausteinen NET.1.1 *Netzarchitektur und -design* bzw. NET.3.2 *Firewall*.

Der Baustein behandelt grundsätzliche Aspekte, die für die Bereitstellung von Webinhalten wichtig sind. Dynamische Inhalte, die durch Webanwendungen bereitgestellt werden, sind nicht Gegenstand des vorliegenden Bausteins. Diese werden im Baustein APP.3.1 *Webanwendungen und Webservices* behandelt. Ebenso werden hier keine Webservices betrachtet.

Webbrowser werden in diesem Baustein nicht betrachtet. Anforderungen dazu sind im Baustein APP.1.2 *Webbrowser* zu finden.

In der Regel werden die Verbindungen zu Webservern verschlüsselt. Der Baustein CON.1 *Kryptokonzept* beschreibt, wie die dazu notwendigen kryptografischen Schlüssel sicher verwaltet werden können.

Werden Webserver nicht selbst betrieben, sondern über einen Hosting-Anbieter bereitgestellt, ist der Baustein OPS.2.3 *Nutzung von Outsourcing* zu beachten.

Oft werden Authentisierungsmechanismen für Webserver verwendet. Ergänzende Anforderungen dazu finden sich im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*.

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.3.2 *Webserver* von besonderer Bedeutung.

2.1. Reputationsverlust

Gelingt es bei einem Angriff mit administrativen Rechten auf einen Webserver zuzugreifen, kann darüber eine manipulierte Webseite ausgeliefert werden (Defacement). So kann die Reputation der Institution geschädigt werden. Ebenso kann die Veröffentlichung falscher Informationen, wie zum Beispiel fehlerhafter Produktbeschreibungen, dazu führen, dass die Reputation der Institution in der Öffentlichkeit leidet. Auch kann die Institution abgemahnt werden, wenn auf ihrer Webseite Inhalte veröffentlicht werden, die gegen gesetzliche Vorschriften verstoßen. Ein Schaden kann auch entstehen, wenn die Webseite nicht verfügbar ist und potenzielle Kunden und Kundinnen deshalb zu Mitbewerbern wechseln.

2.2. Manipulation des Webservers

Bei einem Angriff könnten sich unberechtigte Personen Zugriff auf einen Webserver verschaffen und dessen Dateien manipulieren. Es könnte beispielsweise die Konfiguration der Webserver-Software geändert werden, Schadsoftware verbreitet oder Webinhalte modifiziert werden.

2.3. Denial of Service (DoS)

Durch DoS-Angriffe lässt sich die Verfügbarkeit eines Webangebotes gezielt beeinträchtigen, indem beispielsweise einzelne Accounts durch fehlerhafte Anmeldungen gesperrt werden.

Durch DDoS (Distributed Denial of Service)-Angriffe kann ein Webserver teilweise oder auch ganz ausfallen. Für Clients ist das Webangebot dann nur noch sehr langsam oder gar nicht mehr verfügbar. Für viele Institutionen kann ein solcher Ausfall schnell geschäftskritisch werden, z. B. für Online-Shops.

2.4. Verlust vertraulicher Daten

Viele Webserver verwenden noch veraltete kryptografische Verfahren wie RC4 oder SSL. Eine unzureichende Authentisierung bzw. eine ungeeignete Verschlüsselung kann dazu führen, dass die Kommunikation zwischen den Clients und den Webservern mitgelesen oder manipuliert werden kann. Das gleiche gilt für die Kommunikation zwischen dem Webserver und anderen Servern, wie z. B. Load Balancern.

2.5. Verstoß gegen Gesetze oder Regelungen

Für die Veröffentlichung von Webinhalten gibt es verschiedene regulatorische Anforderungen. Neben den Regelungen der Telemedien- und Datenschutzgesetze, sind auch die Regeln des Urheberrechts zu beachten. Verstöße gegen diese Gesetze können rechtliche Konsequenzen nach sich ziehen.

2.6. Fehlende oder mangelhafte Fehlerbehebung

Treten während des Betriebs eines Webservers Fehler auf, kann sich das z. B. auf dessen Verfügbarkeit auswirken. Auch werden eventuell Inhalte unvollständig dargestellt oder Sicherheitsmechanismen fallen aus. Werden Fehler nicht korrekt behandelt, sind sowohl der Betrieb als auch der Schutz der Funktionen und Daten eines Webservers nicht mehr gewährleistet.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.2 *Webserver* 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	Fachverantwortliche, Compliance-Beauftragte, Zentrale Verwaltung

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.3.2.A1 Sichere Konfiguration eines Webservers (B)

Nachdem der IT-Betrieb einen Webserver installiert hat, MUSS er eine sichere Grundkonfiguration vornehmen. Dazu MUSS er insbesondere den Webserver-Prozess einem Konto mit minimalen Rechten zuweisen. Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Ist dies nicht möglich, SOLLTE jeder Webserver auf einem eigenen physischen oder virtuellen Server ausgeführt werden.

Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden. Nicht benötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden.

APP.3.2.A2 Schutz der Webserver-Dateien (B)

Der IT-Betrieb MUSS alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, so schützen, dass sie nicht unbefugt gelesen und geändert werden können.

Es MUSS sichergestellt werden, dass Webanwendungen nur auf einen definierten Verzeichnisbaum zugreifen können (WWW-Wurzelverzeichnis). Der Webserver MUSS so konfiguriert sein, dass er nur Dateien ausliefert, die sich innerhalb des WWW-Wurzelverzeichnisses befinden.

Der IT-Betrieb MUSS alle nicht benötigten Funktionen, die Verzeichnisse auflisten, deaktivieren. Vertrauliche Daten MÜSSEN vor unberechtigtem Zugriff geschützt werden. Insbesondere MUSS der IT-Betrieb sicherstellen, dass vertrauliche Dateien nicht in öffentlichen Verzeichnissen des Webservers liegen. Der IT-Betrieb MUSS regelmäßig überprüfen, ob vertrauliche Dateien in öffentlichen Verzeichnissen gespeichert wurden.

APP.3.2.A3 Absicherung von Datei-Uploads und -Downloads (B)

Alle mithilfe des Webservers veröffentlichten Dateien MÜSSEN vorher auf Schadprogramme geprüft werden. Es MUSS eine Maximalgröße für Datei-Uploads spezifiziert sein. Für Uploads MUSS genügend Speicherplatz reserviert werden.

APP.3.2.A4 Protokollierung von Ereignissen (B)

Der Webserver MUSS mindestens folgende Ereignisse protokollieren:

- erfolgreiche Zugriffe auf Ressourcen,
- fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Server-Fehlern sowie
- allgemeine Fehlermeldungen.

Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.

APP.3.2.A5 Authentisierung (B)

Wenn sich Clients mit Hilfe von Passwörtern am Webserver authentisieren, MÜSSEN diese kryptografisch gesichert und vor unbefugtem Zugriff geschützt gespeichert werden.

APP.3.2.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote (B) [Fachverantwortliche, Zentrale Verwaltung, Compliance-Beauftragte]

Werden über den Webserver Inhalte für Dritte publiziert oder Dienste angeboten, MÜSSEN dabei die relevanten rechtlichen Rahmenbedingungen beachtet werden. Die Institution MUSS die jeweiligen Telemedien- und Datenschutzgesetze sowie das Urheberrecht einhalten.

APP.3.2.A11 Verschlüsselung über TLS (B)

Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, SOLLTEN diese auf so wenige Fälle wie möglich beschränkt werden.

Wenn eine HTTPS-Verbindung genutzt wird, MÜSSEN alle Inhalte über HTTPS ausgeliefert werden. Sogenannter Mixed Content DARF NICHT verwendet werden.

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.3.2.A8 Planung des Einsatzes eines Webservers (S)

Es SOLLTE geplant und dokumentiert werden, für welchen Zweck der Webserver eingesetzt und welche Inhalte er bereitstellen soll. In der Dokumentation SOLLTEN auch die Informationen oder Dienstleistungen des Webangebots und die jeweiligen Zielgruppen beschrieben werden. Für den technischen Betrieb und die Webinhalte SOLLTEN geeignete Zuständige festgelegt werden.

APP.3.2.A9 Festlegung einer Sicherheitsrichtlinie für den Webserver (S)

Es SOLLTE eine Sicherheitsrichtlinie erstellt werden, in der die erforderlichen Maßnahmen und Zuständigkeiten benannt sind. Weiterhin SOLLTE geregelt werden, wie Informationen zu aktuellen Sicherheitslücken besorgt werden. Auch SOLLTE geregelt werden, wie Sicherheitsmaßnahmen umgesetzt werden und wie vorgegangen werden soll, wenn Sicherheitsvorfälle eintreten.

APP.3.2.A10 Auswahl eines geeigneten Webhosters (S)

Betreibt die Institution den Webserver nicht selbst, sondern nutzt Angebote externer Unternehmen im Rahmen von Webhosting, SOLLTE die Institution bei der Auswahl eines geeigneten Webhosters auf folgende Punkte achten:

- Es SOLLTE vertraglich geregelt werden, wie die Dienste zu erbringen sind. Dabei SOLLTEN Sicherheitsaspekte innerhalb des Vertrags schriftlich in einem Service Level Agreement (SLA) festgehalten werden.
- Die eingesetzten IT-Systeme SOLLTEN vom Webhoster regelmäßig kontrolliert und gewartet werden. Der Webhoster SOLLTE dazu verpflichtet werden, bei technischen Problemen oder einer Kompromittierung von Kundschaftssystemen zeitnah zu reagieren.
- Der Webhoster SOLLTE grundlegende technische und organisatorische Maßnahmen umsetzen, um seinen Informationsverbund zu schützen.

APP.3.2.A12 Geeigneter Umgang mit Fehlern und Fehlermeldungen (S)

Aus den HTTP-Informationen und den angezeigten Fehlermeldungen SOLLTEN weder der Produktname noch die verwendete Version des Webserver ersichtlich sein. Fehlermeldungen SOLLTEN keine Details zu Systeminformationen oder Konfigurationen ausgeben. Der IT-Betrieb SOLLTE sicherstellen, dass der Webserver ausschließlich allgemeine Fehlermeldungen ausgibt, die Clients darauf hinweisen, dass ein Fehler aufgetreten ist. Die Fehlermeldung SOLLTE ein eindeutiges Merkmal enthalten, das es dem IT-Betrieb ermöglicht, den Fehler nachzuvollziehen. Bei unerwarteten Fehlern SOLLTE sichergestellt sein, dass der Webserver nicht in einem Zustand verbleibt, in dem er anfällig für Angriffe ist.

APP.3.2.A13 Zugriffskontrolle für Webcrawler (S)

Der Zugriff von Webcrawlern SOLLTE nach dem Robots-Exclusion-Standard geregelt werden. Inhalte SOLLTEN mit einem Zugriffsschutz versehen werden, um sie vor Webcrawlern zu schützen, die sich nicht an diesen Standard halten.

APP.3.2.A14 Integritätsprüfungen und Schutz vor Schadsoftware (S)

Der IT-Betrieb SOLLTE regelmäßig prüfen, ob die Konfigurationen des Webserver und die von ihm bereitgestellten Dateien noch integer sind und nicht durch Angriffe verändert wurden. Die zur Veröffentlichung vorgesehenen Dateien SOLLTEN regelmäßig auf Schadsoftware geprüft werden.

APP.3.2.A16 Penetrationstest und Revision (S)

Webserver SOLLTEN regelmäßig auf Sicherheitsprobleme hin überprüft werden. Auch 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.3.2.A20 Benennung von Anzusprechenden (S) [Zentrale Verwaltung]

Bei umfangreichen Webangeboten SOLLTE die Institution zentrale Anzusprechende für die Webangebote bestimmen. Es SOLLTEN Prozesse, Vorgehensweisen und Zuständige für Probleme oder Sicherheitsvorfälle benannt werden.

Die Institution SOLLTE eine Kontaktmöglichkeit auf ihrer Webseite veröffentlichen, über die Sicherheitsprobleme an die Institution gemeldet werden können. Für die Behandlung von externen Sicherheitsmeldungen SOLLTE die Institution Prozesse definieren.

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.3.2.A15 Redundanz (H)

Webserver SOLLTEN redundant ausgelegt werden. Auch die Internetanbindung des Webserver und weiterer IT-Systeme, wie etwa der Webanwendungsserver, SOLLTEN redundant ausgelegt sein.

APP.3.2.A17 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.3.2.A18 Schutz vor Denial-of-Service-Angriffen (H)

Der Webserver SOLLTE ständig überwacht werden. Des Weiteren SOLLTEN Maßnahmen definiert und umgesetzt werden, die DDoS-Angriffe verhindern oder zumindest abschwächen.

APP.3.2.A19 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende weiterführende Dokumente veröffentlicht, die für den Betrieb von Webservern relevant sein können:

- Migration auf TLS 1.2 - Handlungsleitfaden
- Sicheres Webhosting: Handlungsempfehlung für Webhoster
- Sicheres Bereitstellen von Webangeboten (ISi-Webserver)

Das National Institute of Standards and Technology (NIST) stellt in seinem Dokument „Guideline on Securing Public Web Servers“ Hinweise zur Absicherung von Webservern zur Verfügung.