|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Webserver"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300050 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Webserver" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc82458236)

[Dokumentenhistorie 3](#_Toc82458237)

[Inhaltsverzeichnis 4](#_Toc82458238)

[Allgemeine Festlegungen 5](#_Toc82458239)

[Ziel / Zweck 5](#_Toc82458240)

[Geltungsbereich 5](#_Toc82458241)

[Zuständigkeiten 5](#_Toc82458242)

[Genehmigungs- und Änderungsverfahren 6](#_Toc82458243)

[Aufbau des Dokuments 6](#_Toc82458244)

[Sicherheitsrichtlinie „Webserver" 7](#_Toc82458245)

[Basismaßnahmen 7](#_Toc82458246)

[Sichere Konfiguration eines Webservers (APP.3.2.A1) 7](#_Toc82458247)

[Schutz der Webserver-Dateien (APP.3.2.A2) 7](#_Toc82458248)

[Absicherung von Datei-Uploads und –Downloads (APP.3.2.A3) 7](#_Toc82458249)

[Protokollierung von Ereignissen (APP.3.2.A4) 7](#_Toc82458250)

[Authentisierung (APP.3.2.A5) 8](#_Toc82458251)

[Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (APP.3.2.A6) 8](#_Toc82458252)

[Rechtliche Rahmenbedingungen für Webangebote (APP.3.2.A7) 8](#_Toc82458253)

[Standardmaßnahmen 8](#_Toc82458254)

[Planung des Einsatzes eines Webservers (APP.3.2.A8) 8](#_Toc82458255)

[Auswahl eines geeigneten Webhosters (APP.3.2.A10) 9](#_Toc82458256)

[Verschlüsselung über TLS (APP.3.2.A11) 9](#_Toc82458257)

[Geeigneter Umgang mit Fehlern und Fehlermeldungen (APP.3.2.A12) 9](#_Toc82458258)

[Zugriffskontrolle für Webcrawler (APP.3.2.A13) 10](#_Toc82458259)

[Integritätsprüfungen und Schutz vor Schadsoftware (APP.3.2.A14) 10](#_Toc82458260)

[Penetrationstest und Revision (APP.3.2.A16) 10](#_Toc82458261)

[Maßnahmen bei erhöhtem Schutzbedarf 11](#_Toc82458262)

[Redundanz (APP.3.2.A15 - A) 11](#_Toc82458263)

[Erweiterte Authentisierungsmethoden für Webserver (APP.3.2.A17 - CI) 11](#_Toc82458264)

[Schutz vor Denial-of-Service-Angriffen (APP.3.2.A18 - A) 11](#_Toc82458265)

[Einrichtung eines Internet-Redaktionsteams (APP.3.2.A19 - CIA) 11](#_Toc82458266)

# Allgemeine Festlegungen

## Ziel / Zweck

Ein Webserver ist die Kernkomponente jedes Webangebotes der <Institution>. Denn ein Webserver nimmt Anfragen der Clients über einen Browser entgegen und liefert die angefragten Inhalte zurück. In den meisten Situationen erfolgt die Kommunikation und Auslieferung der Daten über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS). Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Benutzern bieten, werden sie auch häufig für interne Informationen und Anwendungen im Netz der <Institution> eingesetzt.

Viele Geschäftstätigkeiten der <Institution> sind direkt oder indirekt an die ordnungsgemäße und sichere Funktion eines Webservers gekoppelt. Hieraus ableitend wurden im Rahmen der Entwicklung dieser Sicherheitsrichtlinie geeignete Maßnahmen zur Absicherung für den Betrieb erhoben und in diesem Dokument definiert.

Ziel dieser Sicherheitsrichtlinie ist der sichere Betrieb von Webservern sowie die sichere Bereitstellung von Informationen. Dynamische Bereitstellung von Webinhalten ist nicht Bestandteil dieser Sicherheitsrichtlinie. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines APP.3.2 „Webserver" beachtet.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Webserver“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Webserver"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Sichere Konfiguration eines Webservers (APP.3.2.A1)

Nach der Installation von Webservern werden auf diesen eine sichere Grundkonfiguration vorgenommen. Die <Institution> stellt sicher, dass im Rahmen des Webserver-Prozesses ein Benutzerkonto mit minimalen Rechten verwendet wird. Webserver werden in einer gekapselten Umgebung ausgeführt, insofern dies durch das Betriebssystem bzw. des Containers des Webservers unterstützt wird. Die <Institution> gewährleistet, dass Webserver-Dienste nicht über unnötige Schreibberechtigungen verfügen und nicht benötigte Module sowie Funktionen des Webservers deaktiviert werden. Ebenfalls stellt die <Institution> sicher, dass durch das stetige Sichern von Windows Events bzw. von Syslogs das eigentliche System nicht zum Stillstand kommt.

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

Skripte, Konfigurationsdateien und alle sonstigen Dateien auf Webservern werden durch angemessene Maßnahmen vor unberechtigter Einsicht oder Veränderung geschützt.

Ferner wird sichergestellt, dass Webserver-Anwendungen nur auf Dateien zugreifen können, die sich innerhalb eines definierten Verzeichnisbaumes (WWW-Wurzelverzeichnis) befinden. Die <Institution> stellt sicher, dass jegliche Ressourcen, die sich außerhalb des WWW-Verzeichnisses befinden, nicht aus diesem heraus verlinkt oder verknüpft werden.

Jegliche Funktionen, die Verzeichnisse auflisten, werden deaktiviert. Dateien, die nicht verändert werden sollen, werden schreibgeschützt abgespeichert. Vertrauliche Dateien werden verschlüsselt gespeichert und übertragen.

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

Jegliche Dateien, die durch Webserver bereitgestellt werden, werden hinsichtlich möglicher Schadprogramme durch die etablierte Anti-Malware-Infrastruktur der <Institution> überprüft. Restinformationen werden von jedem Dokument entfernt. Die <Institution> gewährleistet außerdem, dass abrufbare Dateien auf einer separaten Partition vom Storage gespeichert werden.

Für den Datei-Upload auf den Webserver wird eine Maximalgröße festgelegt. Dabei wird sichergestellt, dass für den Upload genügend Speicherplatz reserviert wird.

### Protokollierung von Ereignissen (APP.3.2.A4)

Alle Webserver der <Institution> protokollieren mindestens die folgenden Ereignisse:

* Erfolgreiche Zugriffe auf Ressourcen,
* Fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung,
* fehlenden Ressourcen oder Server-Fehlern sowie
* Allgemeine Fehlermeldungen

Die Protokollierungsdaten werden durch die <Institution> regelmäßig ausgewertet und zentral vorgehalten.

### Authentisierung (APP.3.2.A5)

Für die Authentisierung von Clients (Benutzer und Administratoren) am Webserver werden verschlüsselte Verbindungen (Minimum TLSv1.2) genutzt und die Integrität des Benutzers durch eine integrierte zwei Faktor-Authentisierung (2FA) sichergestellt. Sollten hierfür Passwortdateien auf dem Webserver verwendet werden, sind die Passwörter gemäß den kryptographischen Vorgaben verschlüsselt zu speichern und vor unberechtigten Zugriff zu schützen.

### Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (APP.3.2.A6)

Die Verantwortlichen für die betriebenen Webserver müssen sich aktiv über bekannt gewordene Schwachstellen in der eingesetzten Webserver-Software informieren und sicherheitsrelevante Updates zeitnahe implementieren. Die <Institution> stellt sicher, dass Software-Updates und Patches für den Webserver und den darauf verwendeten Anwendungen und Erweiterungen ausschließlich aus vertrauenswürdigen Quellen bezogen werden. Updates und Patches werden vor ihrer Implementierung angemessen getestet und überprüft. Bei der Ausführung von Patches und Updates wird durch die Verwendung von Datensicherungen und Rücksprungpunkten sichergestellt, dass der ursprüngliche Zustand eines Webservers wiederhergestellt werden kann.

### Rechtliche Rahmenbedingungen für Webangebote (APP.3.2.A7)

Insofern über den Webserver Inhalte und Dienste an Dritte bereitgestellt werden, beachtet die <Institution> die entsprechenden rechtlichen Rahmenbedingungen. In diesem Zusammenhang werden außerdem Anforderungen an die Barrierefreiheit gemäß Behindertengleichstellungsgesetz berücksichtigt.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Planung des Einsatzes eines Webservers (APP.3.2.A8)

Zur Festlegung angemessener Sicherheitsmaßnahmen wird für Webserver geplant und dokumentiert, für welchen Zweck er eingesetzt und wie er in die On-Premise oder Cloud-Infrastruktur integriert wird. Aus der Dokumentation des Webservers geht hervor, welche Informationen und Dienste der Webserver welchen Zielgruppen bereitstellt. Für den technischen Betrieb und die Inhalte des Webservers werden in diesem Zusammenhang die verantwortlichen Mitarbeiter festgelegt.

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

Insofern der Webserver nicht durch die <Institution> selbst betrieben wird, sondern ein externer Dienstleister genutzt wird, berücksichtigt die <Institution> bei der Auswahl des Dienstleisters die folgenden Anforderungen:

* Mit dem Dienstleister wird vertragliche festgelegt, in welcher Form Dienste erbracht werden. Insbesondere Sicherheitsaspekte werden dabei in Form von Service Level Agreements (SLA) vertraglich festgehalten.
* Mit dem Dienstleister wird vertraglich festgelegt, in welcher Form Dienste in Notfall-Situationen wiederhergestellt werden. Insbesondere Aspekte der Wiederherstellungszeit nach Ausfall/Servicebeeinträchtigung (RTO), des maximal tolerierbaren Notbetriebs (MTN) sowie der Datensicherung (RPO) werden vertraglich festgehalten.
* Die Basisinstallation aller angebotenen Produkte muss sicher gestaltet werden. Insofern zusätzliche Anwendungen und Erweiterungen (Plug-Ins) notwendig sind, muss der Dienstleister über potenzielle Risiken informieren. Der Dienstleister muss der <Institution> außerdem proaktiv auf Updates hinweisen.
* Die zur Diensterbringung benötigten IT-Systemen sind regelmäßig vom Dienstleister zu überprüfen und zu warten. Der Dienstleister ist dazu zu verpflichten, bei technischen Problemen oder Kompromittierung von Kundensystemen unverzüglich zu reagieren und die <Institution> hierüber zu informieren.
* Der Dienstleister hat angemessene technische und organisatorische Maßnahmen zum Schutz seiner Infrastrukturen umzusetzen.

### Verschlüsselung über TLS (APP.3.2.A11)

Die <Institution> stellt sicher, dass der Webserver für jegliche Verbindungen eine TLS-Verschlüsselung (HTTPS) basierend auf den intern freigegebenen Protokollen und Algorithmen anbietet. Alle Inhalte des Webservers werden über HTTP Strict Transport Security (HSTS) zur Verfügung gestellt. In diesem Kontext wird ebenso gewährleistet, dass Mixed Content nicht verwendet wird. Kritische Tätigkeiten, wie bspw. die Anmeldung bei einer Webanwendung, erfolgen zwingend über HTTPS.

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

Die folgenden HTTP-Header Konfigurationsmöglichkeiten werden mit geeigneten Parametern hinterlegt:

* Strict-Transport-Security (empfohlen "Strict-Transport-Security: max-age=31536000; includeSubDomains")
* Content Security Policy (Whitelisting von zugelassenen Quellen bspw. "Content-Security-Policy: script-src 'self")
* X-Frame-Options (empfohlen "X-Frame-Options: SAMEORIGIN")
* X-Content-Type-Options (empfohlen "X-Content-Type-Options: nosniff")
* X-XSS-Protection (empfohlen "X-XSS-Protection: 1; mode=block")
* Referrer-Policy (Die Konfiguration kann mit dem Online-Tool <https://report-uri.io/home/generate> erstellt werden)
* Feature-Policy (Möglichkeiten der Konfiguration können über diesen Link <https://github.com/w3c/webappsec-feature-policy/blob/master/README.md> und <https://w3c.github.io/webappsec-feature-policy/> nachgelesen werden)
* X-Powered-By (Hier dürft ihr dann auch gerne kreativ werden)

Die vorgenommenen Einstellungen sollten mit Hilfe dieser Tools <https://securityheaders.com>, <https://webbkoll.dataskydd.net>, <https://observatory.mozilla.org/> und <https://csp-evaluator.withgoogle.com/> verifiziert werden.

HTTP-Informationen und Fehlermeldungen des Webservers werden so ausgerichtet, dass sie keine Informationen über den Namen und die Version der Webserver-Software zur Verfügung stellen. Die <Institution> stellt sicher, dass aus anwendungsspezifischen Fehlermeldungen des Webservers ausschließlich Informationen für den Benutzer hervorgehen. Insofern sich dennoch unerwartete Fehler ergeben, wird gewährleistet, dass der Webserver in einen sicheren Zustand übergeht.

### Zugriffskontrolle für Webcrawler (APP.3.2.A13)

Der Zugriff von Webcrawlern wird nach dem Robots-Exclusion-Standard geregelt. Inhalte sind mit einem Zugriffsschutz zu versehen werden (siehe Abschnitt Authentisierung), um sie vor Webcrawlern zu schützen, die sich nicht an diesen Standard halten.

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

Durch regelmäßige Überprüfungen stellt die <Institution> sicher, dass Dateien und Webinhalte integer sind und nicht durch Angreifer manipuliert wurden. Die Dateien werden außerdem regelmäßig auf Schadsoftware durch die Einbindung in die etablierte Anti-Malware-Infrastruktur überprüft.

### Penetrationstest und Revision (APP.3.2.A16)

Die Webserver der <Institution> werden regelmäßig mindestens alle zwei Jahre einem Penetrationstest unterzogen. Die dafür notwendigen Maßnahmen und Tätigkeiten werden ausschließlich von dafür qualifizierten, zuverlässigen und vertrauenswürdigen Mitarbeitern oder Dienstleistern ausgeführt.

Die <Institution> trifft bereits im Vorfeld mit allen Auftragnehmern und Kunden des Webservice detaillierte Vereinbarungen zur Durchführung und Auswertung des Penetrationstests. Die <Institution> gewährleistet, dass vor der Durchführung eines Penetrationstests das Einverständnis aller zuständigen Stellen vorliegt. Über angemessene Maßnahmen wird sichergestellt, dass innerhalb des Testzeitraums die jeweiligen Ansprechpartner verbindlich feststehen und erreichbar sind. Die Ergebnisse des Penetrationstests werden als vertraulich behandelt und durch angemessene Sicherheitsmaßnahmen geschützt.

Dem <Informationssicherheitsbeauftragter> der <Institution> wird im Anschluss ein Abschlussbericht vorgelegt, welche dieser anschließend in die etablierten Audit- und Risikobewertungsprozesse aufnimmt.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Redundanz (APP.3.2.A15 - A)

Webserver, die Internetanbindung des Webservers sowie sonstige notwendigen IT-Systeme werden redundant ausgelegt.

### Erweiterte Authentisierungsmethoden für Webserver (APP.3.2.A17 - CI)

Für Webserver werden erweiterte Authentisierungsmethoden, wie z. B. beidseitige Zertifikats-basierte Authentisierung oder Mehr-Faktor-Authentifizierung, verwendet.

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

Zur frühzeitigen Identifizierung von Denial-of-Service-Angriffen werden Webserver kontinuierlich überwacht. Die <Institution> definiert und implementiert zusätzliche Maßnahmen, die solche Angriffe verhindern oder abschwächen.

### Einrichtung eines Internet-Redaktionsteams (APP.3.2.A19 - CIA)

Zur Pflege des Webangebots richtet die <Institution> eine eigenständige Internetredaktion ein, welche alle Verantwortlichkeiten für das Webangebot berücksichtigt. Bei umfangreichen Webangeboten wird zusätzlich ein Ansprechpartner für die Webanwendungen festgelegt. Für den Fall von Problemen und Sicherheitsvorfällen werden zusätzliche Prozesse, Vorgehensweisen und Verantwortlichkeiten etabliert werden.