



WEBSEITEN, WEBANWENDUNGEN UND CLOUD-DIENSTE

Verfasser/in	Unternehmenssicherheit
Art der Regelung	Ausführungsbestimmung
Nummer	V00338
Zielgruppe	IT-Mitarbeiter*innen, Projekt- und Produktverantwortliche
Geltungsdauer	Ab Juni 2025
Stand	Juni 2025

ZIEL UND REGELUNGSGEGENSTAND

Das Goethe-Institut betreibt eine Reihe von unterschiedlichen Webanwendungen. Die Sicherheit der Anwendungen hängt zum großen Teil von der Art der Entwicklung und der Implementierung ab. Diese Ausführungsbestimmung beschreibt die Vorgaben, um eine Web-Anwendung entsprechend dem aktuellen Stand der Technik sicher zu entwickeln und zu implementieren. Des Weiteren beinhaltet diese Ausführungsbestimmung Anforderungen für den gesamten Lebenszyklus der Nutzung von Cloud-Diensten sowie die Festlegungen zum Informationssicherheits-Prozess bei Cloud-Diensten selbst.

Abgrenzung

Diese Ausführungsbestimmung macht Vorgaben für die technischen und organisatorischen Vorgaben für Webanwendungen und Clouddienste. Zusätzlich sind typischerweise Vorgaben der Ausführungsbestimmung zur Dienstleistersteuerung und weiterer in den Anlagen referenzierter Dokumente zu beachten.

1 Inhalt

2	Einleitung.....	Fehler! Textmarke nicht definiert.
3	Webanwendung	3
3.1	Sichere Konfiguration von Webanwendungen	5
3.2	Authentisierung.....	5
3.3	Session Management	6
3.4	Einbinden von Inhalten.....	6
3.5	Schutz von Informationen	6
3.6	Schutz vor unerlaubter automatisierter Nutzung.....	7
3.7	Eingabevalidierung und Ausgabekodierung.....	7
3.8	Validierung	8
3.9	Schutz vor unerlaubter automatisierter Nutzung.....	8
3.10	HTTP-Konfiguration	8
3.11	Anbindung von Hintergrundsystemen.....	9
3.12	Einsatz von Web Application Firewalls	9
3.13	Fehlerbehandlung.....	9
4	Einführung eines Cloud-Dienstes.....	10
4.1	Cloud-Strategie.....	10
4.2	Grundsätze für die Nutzung externer Cloud-Dienste.....	11
4.3	Planung.....	12
4.4	Beschaffung.....	14
4.5	Test und Freigabe	14
4.6	Einsatz und laufender Betrieb.....	15
4.7	Beendigung und Außerbetriebnahme.....	15
5	Anlagen.....	16

2 WEBANWENDUNG

Für jede Webanwendung ist gemäß den Vorgaben der Ausführungsbestimmung Informationssicherheitskonzept [1] zu prüfen, ob ein Informationssicherheitskonzept erstellt werden muss.

Bei der Planung der Systemarchitektur ist darauf zu achten, dass neben den Sicherheitsaspekten auch die Geschäftslogik exakt dokumentiert und umgesetzt wird.

Je nach Umfang des Vorhabens sind geeignete Rollen für folgende fachlichen Themen zu definieren:

- Requirements-Engineering (Anforderungsmanagement) und Änderungsmanagement,
- Software-Entwurf und -Architektur,
- Informationssicherheit in der Software-Entwicklung,
- Software-Implementierung in dem für das Entwicklungsvorhaben relevanten Bereichen,
- Software-Tests.

Für die Entwicklung einer Webanwendung muss ein geeignetes Vorgehensmodell festgelegt werden. Anhand des gewählten Modells ist ein Ablaufplan zu erstellen, wobei die Sicherheitsanforderungen integriert werden. Das gewählte Vorgehensmodell, einschließlich der festgelegten Sicherheitsanforderungen müssen eingehalten werden.

Zur Auswahl einer Entwicklungsumgebung müssen erforderliche und optionale Kriterien definiert werden, wobei die Sicherheitsanforderungen auch in dieser Umgebung zu berücksichtigen sind.

Die Produktiv-, Test- und Entwicklungsumgebungen sind auf getrennten Systemen zu betreiben. Auf Testsystemen sollten nach Möglichkeit keine Produktivdaten verwendet werden. Testdaten müssen ggf. anonymisiert oder pseudonymisiert werden. In den verschiedenen Umgebungen müssen unterschiedliche Zugangsdaten gewählt werden. Cyber-Angriffe auf die Entwicklungs- oder Testumgebung dürfen keine Auswirkungen auf die Produktivumgebung haben.

Wird im Rahmen des Entwicklungs- und Implementierungsprozesses auf externe Bibliotheken zurückgegriffen, müssen diese aus vertrauenswürdigen Quellen bezogen werden. Bevor externe Bibliotheken verwendet werden, muss deren Integrität sichergestellt werden.

Schon bevor die Webanwendung im Freigabeprozess getestet und freigegeben wird, sind entwicklungsbegleitende Software-Tests durchzuführen und der Quellcode muss auf Fehler gesichtet werden.

Die entwicklungsbegleitenden Tests müssen die funktionalen und nichtfunktionalen Anforderungen der Webanwendung umfassen. Die Tests sollten dabei auch Negativtests abdecken. Zusätzlich sind alle kritischen Grenzwerte der Eingabe sowie der Datentypen zu überprüfen.

Es ist sicherzustellen, dass sicherheitskritische Patches und Updates für die entwickelte Webanwendung zeitnah durch die Entwickler*innen bereitgestellt werden. Werden für verwendete externe Bibliotheken sicherheitskritische Updates bereitgestellt, dann müssen die Entwickler*innen die Webanwendung hierauf anpassen und entsprechende Patches und Updates zur Verfügung stellen.

Der Quellcode des Webentwicklungsprojekts muss über eine geeignete Versionsverwaltung verfügen. Der Zugriff auf die Versionsverwaltung ist zu regeln, dabei muss festgelegt werden, wann Änderungen am Quellcode durch die Entwickler*innen als eigene Version in der Versionsverwaltung gespeichert werden sollen. Es ist sicherzustellen, dass durch die Versionsverwaltung alle Änderungen am Quellcode nachvollzogen und

rückgängig gemacht werden können. Die Versionsverwaltung ist im Datensicherungskonzept zu berücksichtigen und darf nicht ohne Datensicherung erfolgen.

Es müssen geeignete Projekt-, Funktions- und Schnittstellendokumentationen erstellt und aktuell gehalten werden. Die Betriebsdokumentation muss konkrete Sicherheitshinweise für die Installation und Konfiguration durch die Administration, sowie für die Benutzung der Webanwendung beinhalten.

Die Entwicklung der Webanwendung sollte so dokumentiert sein, dass Fachleute mithilfe der Dokumentation den Programm-Code nachvollziehen und weiterentwickeln können. Die Aspekte zur Dokumentation müssen im gewählten Vorgehensmodell berücksichtigt werden.

Die Softwarearchitektur der Webanwendung muss mit allen Bestandteilen und Abhängigkeiten dokumentiert werden. Die Dokumentation sollte bereits während des Entwicklungsverlaufs aktualisiert und angepasst werden. Die Dokumentation ist so zu gestalten, dass diese schon in der Entwicklungsphase genutzt werden kann und Entscheidungen nachvollziehbar sind.

In der Dokumentation müssen alle für den Betrieb notwendigen Komponenten gekennzeichnet werden, die nicht Bestandteil der Webanwendung sind. Es ist zu beschreiben, welche Komponenten welche Sicherheitsmechanismen umsetzen, wie die Webanwendung in eine bestehende Infrastruktur integriert wird und welche kryptografischen Funktionen und Verfahren eingesetzt werden.

Die Entwickler*innen und die übrigen Mitglieder des Entwicklungsteams müssen zu generellen Informationssicherheitsaspekten und zu den jeweils speziell für sie relevanten Aspekten geschult sein.

Neben den allgemeinen Aspekten zur Beschaffung von Software sollten bei der Beschaffung von Webanwendungen mindestens die folgenden Kriterien berücksichtigt werden:

- 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 die Entwickler*innen der Software,
- Schutzmechanismen vor verbreiteten Angriffen auf Webanwendungen
- Zugriff auf den Quelltext der Webanwendung oder des Webservices.

Bevor eine neue extern erreichbare Webanwendung produktiv geschaltet wird, muss ein Penetrationstest durchgeführt werden, in dem die sicherheitstechnische Umsetzung der Sicherheitsmaßnahmen geprüft wird. Dies gilt auch bei grundlegenden Änderungen.

Die Ergebnisse von Penetrationstests müssen nachvollziehbar dokumentiert, ausreichend geschützt und vertraulich behandelt werden. Abweichungen müssen behoben werden. Die Ergebnisse sind der Informationssicherheit vorzulegen.

2.1 Sichere Konfiguration von Webanwendungen

Webanwendungen und Webservices sind so zu konfigurieren, dass auf ihre Ressourcen und Funktionen ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade zugegriffen werden kann. Der Zugriff auf nicht benötigte Ressourcen und Funktionen muss nach Möglichkeit deaktiviert oder zumindest eingeschränkt werden. Die Zeichenkodierung muss entsprechend konfiguriert werden.

Nach der Installation muss ein Webserver eine sichere Grundkonfiguration erhalten. Dazu muss die Betriebsverantwortliche insbesondere dem Webserver-Prozess ein Konto mit minimalen Rechten zuweisen. Der Webserver sollte nach Möglichkeit in einer gekapselten Umgebung ausgeführt werden. 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 Webserver müssen deaktiviert werden.

Grundsätzlich sollten folgende Ereignisse in der Webanwendung bzw. dem Webserver protokolliert werden:

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

Die Protokollierungsdaten müssen zur regelmäßigen Auswertung zur Verfügung stehen.

Alle mithilfe des Webserver veröffentlichten Dateien müssen zuvor auf Schadprogramme geprüft werden. Es muss regelmäßig überprüft werden, 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 sind regelmäßig auf Schadsoftware zu prüfen.

2.2 Authentisierung

Webanwendungen müssen so konfiguriert werden, dass sich Clients gegenüber der Webanwendung authentisieren müssen, wenn diese auf geschützte Ressourcen zugreifen wollen. Es müssen angemessene Authentisierungsmethode ausgewählt werden, mindestens jedoch Benutzername und Passwort. Hierbei sind die Vorgaben der Ausführungsbestimmung Passwörter zu berücksichtigen.

Für interne Webanwendungen sollte nach Möglichkeit eine zentrale Authentisierungskomponente verwendet werden. Diese sollte mit etablierten Standardkomponenten (z. B. aus Frameworks oder Programmbibliotheken) umgesetzt werden. Falls eine Webanwendung Authentisierungsdaten auf einem Client speichert, muss explizit auf die Risiken der Funktion hingewiesen werden und eine Zustimmung erfolgen („Opt-In“).

Die Webanwendung muss die Möglichkeit bieten, Grenzwerte für fehlgeschlagene Anmeldeversuche festzulegen. Bei mehrfacher Falscheingabe des Passwortes muss die Benutzer*in gesperrt werden. Die Sperrung darf erst nach einem entsprechenden Freigabeverfahren wieder rückgängig gemacht werden. Die Webanwendung muss die Benutzer*in sofort informieren, wenn das Passwort zurückgesetzt wurde.

Bei höheren Ansprüchen an Vertraulichkeit oder Integrität sind Mehr-Faktor-Authentisierungsmethoden zu implementieren.

Es muss mittels Autorisierungskomponenten sichergestellt werden, dass die Benutzer*innen ausschließlich Aktionen durchführen können, zu denen sie berechtigt sind. Jeder Zugriff auf geschützte Inhalte und Funktionen muss vor der Ausführung kontrolliert werden. Bei URL-Aufrufen und Objekt-Referenzen muss eine Zugriffskontrolle vorhanden sein, welche bei einem fehlerhaften Zugriff die Anfrage ablehnt.

2.3 Session Management

Session-IDs müssen geeignet geschützt werden sowie zufällig und mit ausreichender Entropie erzeugt werden. Falls das Framework der Webanwendung sichere Session-IDs generieren kann, muss diese Funktion des Frameworks verwendet werden. Sicherheitsrelevante Konfigurationsmöglichkeiten des Frameworks sind zu berücksichtigen. Wenn Session-IDs übertragen und von den Clients gespeichert werden, muss eine ausreichend geschützte Übertragung stattfinden.

Die Webanwendung muss die Möglichkeit bieten, eine bestehende Sitzung explizit zu beenden. Nachdem ein Konto angemeldet wurde, muss eine bereits bestehende Session-ID durch eine neue ersetzt werden. Sitzungen müssen eine maximale Gültigkeitsdauer besitzen (Timeout). Inaktive Sitzungen müssen automatisch nach einer bestimmten Zeit ungültig werden. Nachdem die Sitzung ungültig ist, müssen alle Sitzungsdaten ungültig und gelöscht sein.

2.4 Einbinden von Inhalten

Falls eine Webanwendung oder ein Webservice eine Upload-Funktion für Dateien anbietet, so ist diese Funktion so weit wie möglich einzuschränken. Insbesondere müssen die maximale Dateigröße, erlaubte Dateitypen und erlaubte Speicherorte festgelegt werden. Zudem ist festzulegen, welche Clients die Funktion verwenden dürfen. Zugriffs- und Ausführungsrechte müssen restriktiv gesetzt werden. Es ist sicherzustellen, dass Clients Dateien nur im vorgegebenen erlaubten Speicherort (vorgegebener Pfad) speichern können und den Ablageort nicht beeinflussen können. Auf dem Webserver muss für Uploads genügend Speicherplatz reserviert werden.

Es ist sicherzustellen, dass eine Webanwendung ausschließlich vorgesehene Daten und Inhalte einbindet und ausliefert. Die Ziele der Weiterleitungsfunktion einer Webanwendung müssen ausreichend eingeschränkt werden, sodass ausschließlich auf vertrauenswürdige Webseiten weitergeleitet wird. Falls die Vertrauensdomäne verlassen wird, muss die Webanwendung darüber informieren.

Es ist sicherzustellen, dass vertrauliche Daten von den Clients zu den Servern nur mit der HTTP-Post-Methode übertragen werden.

2.5 Schutz von Informationen

Jeder Zugriff auf geschützte Inhalte und Funktionen muss vor der Ausführung kontrolliert werden. Bei URL-Aufrufen und Objekt-Referenzen muss eine Zugriffskontrolle vorhanden sein, welche bei einem fehlerhaften Zugriff die Anfrage ablehnt.

Durch Direktiven in der Webanwendung ist zu gewährleisten, dass clientseitig keine schützenswerten Daten zwischengespeichert werden. In Formularen dürfen keine vertraulichen Formulardaten im Klartext angezeigt werden. Nach Möglichkeit ist zu verhindern, dass vertrauliche Daten von Webbrowsern unerwartet gespeichert werden.

Sämtliche Zugangsdaten zu Webanwendungen müssen serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden (Salted Hash). Die Dateien mit den Quelltexten der Webanwendung sind vor unerlaubten Abrufen zu schützen.

Es ist sicherzustellen, dass Rückantworten und Fehlermeldungen von Webanwendungen keine Informationen mit Hinweisen auf Sicherheitsmechanismen enthalten. Aus den HTTP-Informationen und den angezeigten Fehlermeldungen dürfen weder der Produktname noch die verwendete Version eines Webserver ersichtlich sein. Fehlermeldungen dürfen keine Details zu Systeminformationen oder Konfigurationen ausgeben. Es ist sicherzustellen, dass der Webserver ausschließlich allgemeine Fehlermeldungen ausgibt. Die Fehlermeldungen sollten ein eindeutiges Merkmal enthalten, welches 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.

Es muss sichergestellt werden, dass alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, so geschützt werden, dass sie nicht unbefugt gelesen und geändert werden können.

Kommentare in Quelltexten (bspw. HTML, Javascript, etc.) dürfen keine Informationen enthalten, die Rückschlüsse auf interne Informationen des Goethe-Instituts, die Anwendungslogik oder die Serverstruktur zulassen. Nach Möglichkeit sind im produktiven Release einer Webanwendung alle Kommentare zu entfernen.

Webanwendungen dürfen nur auf einen definierten Verzeichnisbaum zugreifen (WWW-Wurzelverzeichnis). Der Webserver ist so zu konfigurieren, dass nur Dateien ausgeliefert werden, die sich innerhalb des WWW-Wurzelverzeichnisses befinden. Alle nicht benötigten Funktionen, die Verzeichnisse auflisten, müssen deaktiviert werden.

Vertrauliche Daten müssen vor unberechtigtem Zugriff geschützt werden. Insbesondere muss sichergestellt werden, dass vertrauliche Dateien nicht in öffentlichen Verzeichnissen des Webserver liegen.

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, sind alle Inhalte über HTTPS auszuliefern. Sogenannter Mixed Content darf nicht verwendet werden.

2.6 Schutz vor unerlaubter automatisierter Nutzung

Es müssen Sicherheitsmechanismen implementiert werden, die die Webanwendung vor automatisierten Zugriffen schützen. Bei der Implementierung der Sicherheitsmechanismen ist zu berücksichtigen, wie sich diese auf die Nutzungsmöglichkeiten der berechtigten Konten auswirken.

Nach Möglichkeit sollte der Zugriff von *Webcrawlern* nach dem Robots-Exclusion-Standard geregelt werden. Inhalte sind mit einem Zugriffsschutz zu versehen, um sie vor *Webcrawlern* zu schützen, die sich nicht an diesen Standard halten.

2.7 Eingabevalidierung und Ausgabekodierung

Sämtliche an eine Webanwendung übergebenen Daten sind als potenziell gefährlich zu behandeln und geeignet zu filtern. Eingabedaten sowie Datenströme und Sekundärdaten, wie z. B. Session-IDs, müssen serverseitig validiert werden. Fehleingaben sollten möglichst nicht automatisch behandelt werden

(Sanitizing). Lässt es sich jedoch nicht vermeiden, muss Sanitizing sicher umgesetzt werden. Ausgabedaten sind so zu codieren, dass schadhafter Code auf dem Zielsystem nicht interpretiert oder ausgeführt wird.

2.8 Validierung

Zum Schutz vor SQL-Injection müssen *Stored Procedures* bzw. *Prepared SQL Statements* eingesetzt werden, falls Daten an ein Datenbankmanagementsystem weitergeleitet werden. Ist dies nicht möglich, müssen die *SQL-Queries* separat abgesichert werden.

Sämtliche Eingabeparameter müssen serverseitig durch die Anwendung validiert werden. Dies ist durch die Programmlogik sicherzustellen. Input-Daten sind daraufhin zu filtern, ob sie sicherheitskritische Inhalte enthalten. Folgende Parameter sämtlicher Eingangsdaten sind zu prüfen:

- Länge der Eingabe
- Datentyp
- Vergleich mit der Liste vorgegebener Eingaben
- Quelle der Variable (GET, POST, Cookie)
- Namen von Form-Variablen

Hidden Fields sollten nicht genutzt werden, um vertrauliche Informationen zu transportieren. Diese sind nur geeignet, um dem Client Parameter zu übergeben, die dieser nicht ändern sollt. Die Rückgabewerte des Clients sind zu validieren.

Zeichen oder Zeichenketten, die Browser fälschlicherweise als Code (HTML, JavaScript, ActiveX, usw.) interpretieren, dürfen nicht ausgegeben werden. Diese müssen invalidiert werden, d. h, eine Umwandlung in „*Named Character Reference*“-Darstellung.

Zeichen oder Zeichenketten, die Browser fälschlicherweise als Code (HTML, JavaScript, ActiveX, usw.) interpretieren dürfen nicht ausgegeben werden. Diese müssen invalidiert werden, d. h, eine Umwandlung in „*Named Character Reference*“-Darstellung.

2.9 Schutz vor unerlaubter automatisierter Nutzung

Es ist sicherzustellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei ist zu berücksichtigen, 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, ist dies ebenfalls bei der Konfiguration der Schutzmechanismen zu berücksichtigen.

2.10 HTTP-Konfiguration

Der Webserver muss für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS unter Berücksichtigung der Vorgaben der Ausführungsbestimmung Kryptografie 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, sind alle Inhalte über HTTPS auszuliefern. Sogenannter Mixed Content darf nicht verwendet werden. Nicht benötigte HTTP-Methoden müssen deaktiviert werden.

Zum Schutz vor *Clickjacking*, *Cross-Site-Scripting* und anderen Angriffen müssen geeignete HTTP-Response-Header gesetzt werden. Es sollten mindestens die folgenden HTTP-Header verwendet werden:

- Content-Security-Policy,
- Strict-Transport-Security,
- Content-Type,
- X-Content-Type-Options
- Cache-Control
- X-Frame-Options
- X-XSS-Protection

Die verwendeten HTTP-Header sollten so restriktiv wie möglich sein und auf die Webanwendung abgestimmt werden. Cookies sind grundsätzlich mit den Attributen `secure`, `SameSite` und `httponly` zu setzen.

2.11 Anbindung von Hintergrundsystemen

Der Zugriff auf Hintergrundsysteme, auf denen Funktionen und Daten ausgelagert werden, dürfen ausschließlich über definierte Schnittstellen und von definierten IT-Systemen aus möglich sein. Bei der Kommunikation über Netz- und Standortgrenzen hinweg ist der Datenverkehr zu authentisieren und zu verschlüsseln.

2.12 Einsatz von Web Application Firewalls

Bei erhöhtem Schutzbedarf der Daten sollten Web Application Firewalls (WAF) eingesetzt werden. Die Konfiguration der eingesetzten WAF ist auf die zu schützende Webanwendung oder den Webservice anzupassen. Nach jedem Update der Webanwendung oder des Webservices ist die Konfiguration der WAF zu prüfen.

2.13 Fehlerbehandlung

Treten während der Laufzeit einer Webanwendung Fehler auf, müssen diese so behandelt werden, dass die Webanwendung weiter in einem konsistenten Zustand bleibt. Die Webanwendung muss Fehlermeldungen protokollieren. Falls eine veranlasste Aktion einen Fehler verursacht, sollte die Webanwendung diese Aktion abbrechen. Im Fehlerfall sollte der Zugriff auf eine angeforderte Ressource oder Funktion verweigert werden. Zuvor reservierte Ressourcen sollten im Rahmen der Fehlerbehandlung wieder freigegeben werden. Nach Möglichkeit sollte ein Fehler von der Webanwendung selbst behandelt werden.

3 EINFÜHRUNG EINES CLOUD-DIENSTES

Für jeden Cloud-Dienst muss ein Cloud-Owner benannt werden. Die Verantwortung für die Umsetzung der Phasen Planung, Beschaffung, Test und Freigabe, Einsatz und laufender Betrieb sowie Beendigung und Außerbetriebnahme liegt beim Cloud-Owner.

3.1 Cloud-Strategie

Es müssen der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste [2], der Kriterienkatalog Cloud Computing C5 [3] und die Anforderungen des BSI IT-Grundschutzkompendiums [4] als Ausgangsbasis für die Sicherung von einzelnen Cloud-Diensten herangezogen.

In der Nutzung von Cloud-Diensten sieht das Goethe-Institut das Potenzial, insbesondere die nachfolgend aufgeführten Vorteile für sich zu nutzen:

- Schnelle Bereitstellung von Applikationen: Mit Hilfe von Cloud-Diensten können Bedarfe der Fachbereiche zeitnah erfüllt werden, sofern es sich um Bedarfe nach standardisierten Anwendungen (z.B. Dateiaustauschplattformen, Kollaborationstools) handelt.
- Flexible Skalierbarkeit: Cloud-Dienste lassen sich flexibel an den Ressourcenbedarf der Cloud-Endanwender anpassen (z.B. bei der Bereitstellung öffentlicher Lernmaterialien oder der Durchführung von Onlineprüfungen; insbesondere zu Zeiten hoher Nachfrage)
- Bedarfsgerechte Abrechnung: Abhängig von dem jeweiligen Preismodell sind lediglich die konkret genutzten und verbrauchten Ressourcen zu bezahlen.
- Entlastung des IT-Betriebs: Aufwände für Planung, Aufbau, Betrieb und Management eigener IT-Infrastrukturen lassen sich durch den Einsatz von Cloud-Diensten reduzieren. So kann der IT-Betrieb seine Ressourcen auf die Kern-IT des Goethe-Instituts fokussieren.
- Erreichbarkeit: Die Cloud-Dienste sind in der Regel aus dem Internet für diverse Endgeräte erreichbar. Es ist deshalb keine Verbindung zu einem internen Netz mehr notwendig.

Cloud-Nutzung weist im Allgemeinen mehrere Risiken auf, insbesondere:

- Kontrollverlust: Je nach Servicemodell liegt die Verantwortlichkeit für Sicherheitsmaßnahmen in großen Teilen beim Cloud-Anbieter. Zugleich bleibt der Cloud-Nutzer verantwortlich für die Informationen, die in der Cloud verarbeitet werden.
- Vendor Lock-In: Cloud-Anbieter sind bestrebt, Kunden stark an sich zu binden. Interoperabilität und Exit-Strategien werden dadurch aus Sicht der Cloud-Nutzer erschwert.
- Compliance: Die an Cloud-Anbieter zu stellenden Compliance-Anforderungen oder deren Nachweis können sich im Laufe der Cloud-Nutzung ändern. Dies begünstigt das Auftreten von Compliance-Verstößen, für die letztendlich der Cloud-Nutzer die Verantwortung trägt. Außerdem werden möglicherweise Server für die Verarbeitung der Informationen genutzt, die sich an einem Ort befinden, an dem andere rechtliche Grundlagen vorliegen (z.B. außerhalb der EU).
- Sicherheitsvorfälle: Cloud-Anbieter können aufgrund ihrer Exponiertheit (Public Clouds) und Marktstärke (*Hyperscaler*) ein lohnendes Ziel für Angreifer darstellen. Dadurch können Informationen des Cloud-Nutzers beim Anbieter kompromittiert werden.
- Verfügbarkeit: Ein Ausfall der Internetverbindung beim Goethe-Institut oder eine Störung beim Cloud-Anbieter kann dazu führen, dass ein Zugriff auf die Cloud-Dienste vorübergehend nicht möglich ist.

- Unzureichende Mandantenfähigkeit: Falls Ressourcen mehrerer Cloud-Kunden in einer Cloud-Umgebung nicht ausreichend voneinander getrennt sind, kann es zu Integritäts- oder Vertraulichkeitsverlust der darin verarbeiteten Informationen kommen.
- Unzureichende Planung: In allen Phasen einer Cloud-Nutzung (Anforderungserhebung, Beschaffung, Migration, Integration, Nutzung, Beendigung) kann durch fehlende oder unzureichende Planung die Informationssicherheit in allen Grundwerten beeinträchtigt werden.
- Nutzung der Informationen durch Cloud-Anbieter: Möglicherweise können übertragene Informationen zur Verarbeitung durch den Cloud-Anbieter, beispielsweise zum Trainieren von künstlicher Intelligenz, genutzt werden. In dem Fall können sowohl sensible als auch personenbezogene Informationen missbraucht und unrechtmäßig genutzt werden.

Ausgehend von den Grundaussagen werden nachfolgend Szenarien beschrieben, in denen eine Cloud-Nutzung grundsätzlich möglich bzw. nicht möglich ist.

Für die nachfolgend beschriebenen Szenarien ist die Nutzung von Cloud-Diensten grundsätzlich ausgeschlossen:

- Verarbeitung von hoch schutzbedürftigen Informationen in nicht dafür freigegebenen Clouds

Für die nachfolgend beschriebenen Szenarien ist die Nutzung von Cloud-Diensten, unter Berücksichtigung der Anforderungen dieser Richtlinie, grundsätzlich möglich:

- Verarbeitung von hoch schutzbedürftigen Informationen in dafür freigegebenen Private Clouds, Community Clouds oder Hybrid-Clouds
- Nutzung von Dritten bereitgestellter Cloud-Dienste (z.B. im Rahmen organisationsübergreifender Kooperationen)
- Verarbeitung von geschäftlichen Informationen mit normalen Schutzbedarf hinsichtlich der Vertraulichkeit mittels externer Cloud-Dienste

3.2 Grundsätze für die Nutzung externer Cloud-Dienste

Unabhängig von Service- oder Bereitstellungsmodellen haben potenzielle Cloud-Anbieter des Goethe-Instituts grundlegende Anforderungen an die Informationssicherheit zu erfüllen:

- Der Cloud-Anbieter muss einen dokumentierten und gültigen Nachweis der Informationssicherheit erbringen. Dazu gehört der Nachweis der C5 Konformität oder aber auch der Nachweis eines eigenen Informationssicherheitskonzepts (z.B. nach ISO 27001) inkl. Notfallmanagement/BCM.
- Der Cloud-Anbieter muss an der IT-Sicherheitskonzeption bzw. der Risikoanalyse des Goethe-Instituts mitwirken. Mindestens muss er dabei notwendige Informationen zu liefern.
- Die Nutzung des Cloud-Dienstes darf nicht gegen einzuhaltende rechtliche oder sonstige verbindlich anzuwendenden Randbedingungen Verstoßen (z.B. Datenschutz, sonstiges (lokales) Recht, Mitbestimmung des Betriebsrats, Vergaberecht, Lizenzbedingungen etc.)

Im Sinne der geteilten Verantwortlichkeit obliegt es auch dem Goethe-Institut als Cloud-Nutzer, relevante Anforderungen in seinem Verantwortungsbereich zu erfüllen, insbesondere:

- Das Goethe-Institut muss je Cloud-Nutzung ein IT-Sicherheitskonzept gemäß Vorgaben des ISMS des Goethe-Instituts erstellen und umsetzen [1].

- Abhängig vom Schutzbedarf und der Komplexität des konkreten Nutzungsszenarios kann eine Risikoanalyse oder eine vereinfachte Sicherheitskonzeption vor der Umsetzung der Cloud-Nutzung ausreichend sein. Die Entscheidung hierüber trifft das Informationssicherheits-Management.
- Alle im Rahmen der Cloud-Nutzung für die Verarbeitung im Cloud-Dienst vorgesehenen Informationen in Verantwortlichkeit des Goethe-Instituts müssen im IT-Sicherheitskonzept bzw. der Risikoanalyse berücksichtigt werden. Die Bewertung des Schutzbedarfs dieser Informationen muss gemäß den Vorgaben des ISMS des Goethe-Instituts erfolgen [1].
- Im Rahmen des ISMS muss eine zentrale Übersicht über die eingesetzten Cloud-Dienste sowie der darauf verarbeiteten Informationen und dem jeweiligen Verantwortlichen geführt werden.

Entsprechend der Strategie zur Nutzung externer Cloud-Dienste dürfen nicht alle Informationen in Public-Clouds verarbeitet werden.

Insbesondere Informationen mit einem Schutzbedarf hinsichtlich der Vertraulichkeit von sehr hoch dürfen nicht in einer Public-Cloud verarbeitet werden. Abweichungen von dieser Vorgabe sind durch den Cloud-Owner zu dokumentieren und mit dem Informationssicherheits-Management abzustimmen. Hierbei ist bei personenbezogenen Daten grundsätzlich die Datenschutzbeauftragte (DSB) in den Freigabeprozess zu integrieren.

Für die einzelnen verwendeten Dienste ist abzugrenzen, wer für welchen Anteil (Infrastruktur, Plattform, Software) und dessen sichere Administration sowie operative Bereitstellung verantwortlich ist. Vor der Nutzung muss dabei festgelegt und dokumentiert werden welche Tätigkeiten durch das Goethe-Institut und welche Tätigkeiten durch die Anbieter*in übernommen werden.

Die Nutzung von externen Cloud-Diensten ist durch das Cloud Asset Management in einer zentralen Datenbank zu dokumentieren. Die folgenden Informationen der Cloud-Dienste sind zu erheben und zentral zu sichern:

- Name des Dienstes
- Beschreibung des Dienstes
- Wofür wird der Dienst im Goethe-Institut genutzt
- Adresse (URL)
- Verantwortliche beim Goethe-Institut (Cloud Owner, ggf. Administrator*innen)
- Ansprechpartner*innen bei der Anbieter*in (u.a. für Störungen und Sicherheitsvorfälle/Ereignisse)
- Nutzende Stellen im Goethe-Institut
- In der Cloud verarbeitete Informationen (Schutzbedarf)
- Nutzungszeitraum

Die Informationen sind durch den Cloud-Owner gegenüber dem Cloud Asset Management auf einem aktuellen Stand zu halten und durch das Informationssicherheits-Management regelmäßig zu verifizieren.

3.3 Planung

Die erfolgreiche Implementierung von Cloud-Services erfordert eine sorgfältige Planung, die die spezifischen Anforderungen und Zielsetzungen des Goethe-Instituts berücksichtigt.

Im nächsten Schritt wird der Cloud-Owner definiert. Dieser trägt im Goethe-Institut die Verantwortung für die Gesamtkoordination und Überwachung des Cloud-Einsatzes.

Es ist zu klären, wer die Hauptnutzer des Cloud-Dienstes sind und welche konkreten Zwecke mit der Nutzung verfolgt werden. Hierbei sind alle zu verarbeitenden Informationen zu erheben. Diese Definition bildet die Grundlage zur Entscheidung im Planungsprozess und eine zielgerichtete Konfiguration der Cloud-Ressourcen.

Bei der Auswahl sollen typische Nutzungsszenarien identifiziert werden, um den Kriterien dieser Richtlinie gerecht zu werden. Die bedarfsgerechte Auswahl soll sowohl funktional als auch kosteneffizient erfolgen und beispielsweise die Liste bereits freigegebener Cloud-Dienste des Cloud Asset Managements berücksichtigen.

Im Rahmen der Erstellung des Informationssicherheitskonzepts werden die relevanten Sicherheitsanforderungen definiert. Dabei ist die Einhaltung der geforderten Standards und Vorgaben zu überprüfen. Hierbei erfolgt eine klare Zuordnung der Verantwortlichkeiten zwischen dem Goethe-Institut und dem ausgewählten Cloud-Anbieter.

Im Informationssicherheitskonzepten wird entschieden, ob eine Risikoanalyse für die Cloud-Nutzung durchgeführt werden muss. Die Durchführung der Risikoanalyse erfolgt gemäß den Vorgaben der Ausführungsbestimmung Informationssicherheitskonzept und Risikoanalyse [1]. Diese Analyse bildet die Grundlage für geeignete Sicherheitsmaßnahmen und ermöglicht eine proaktive Risikobewältigung.

Die Entscheidung zur Nutzung bestimmter Cloud-Services wird nach klaren Kriterien getroffen. Die hierzu herangezogenen Kriterien sind angemessen zu dokumentieren. Die Autorisierung erfolgt durch den Cloud-Owner. Dabei wird auch die Finanzierung im Vorfeld geklärt, um Transparenz und Budgetsicherheit zu gewährleisten.

Im Rahmen der Planung werden detaillierte Anforderungen und Vorgaben an den Cloud-Dienst definiert, darunter:

- Vorgaben zum Speicherort der Informationen
- Vorgaben zur sicheren Administration
- Vorgaben zu Betriebs- und Sicherheitsprozessen
- Vorgaben zur Kryptographie (siehe auch [5]**Fehler! Verweisquelle konnte nicht gefunden werden.**)
- Vorgaben zum Identitäts- und Berechtigungsmanagement (siehe auch [6])
- Vorgaben zur Datensicherung

Diese Vorgaben dienen als Grundlage für die Konfiguration und den Betrieb der Cloud-Services.

Insbesondere sind dabei die folgenden Prüffragen zu berücksichtigen:

- Welche Art von Informationen sollen in der Cloud verarbeitet werden?
- Dürfen die Informationen grundsätzlich in einer Cloud verarbeitet werden?
- Gibt es Einschränkungen bzgl. des Speicher- und Verarbeitungsorts (z. B. aufgrund von Zugriff auf die Informationen durch Dritte, Spionage)?

- Ergeben sich daraus Einschränkungen bezüglich des Bereitstellungsmodells (Public Cloud, Community Cloud, Private Cloud oder Hybrid Cloud)?
- Werden die Vorgaben des C5 Kriterienkatalogs eingehalten [3]?
- Wo werden die Informationen gesichert?
- Wo liegt die Gerichtsbarkeit des Dienstes?

3.4 Beschaffung

Dieses Kapitel legt die relevanten Schritte und Vorgaben für den Beschaffungs-Prozess fest. Grundsätzlich sind bei der Beschaffung die „Ergänzenden Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud)“ einzuhalten [7].

Die Auswahl und Beschaffung von Cloud-Services erfolgen auf Basis der in der Planung definierten Kriterien. Diese Kriterien sind auf die spezifischen Bedürfnisse des Goethe-Instituts zugeschnitten und bilden die Grundlage für eine bedarfsgerechte Auswahl.

Vor der Beschaffung soll eine umfassende Wirtschaftlichkeitsbetrachtung und Kosten-Nutzen-Abschätzung durch den Cloud-Owner erfolgen. Dabei sind folgende Aspekte zu berücksichtigen:

- Nutzungskosten des Services inkl. Einrichtung und Betrieb
- Interner Administrationsaufwand
- Schulung von Mitarbeiter*innen/Administrator*innen
- Bedarf an neuer IT oder neuer Netzanbindung
- Kosten/Aufwände bei der Anpassung von Prozessen
- Kosten der Migration
- Interne Einsparungen
- Kosten für die etwaige Umsetzung von Exit-Strategien und Außerbetriebnahmen

Bei der Auswahl von Cloud-Services muss auch ein geeignetes Lizenz- oder Tarifmodell ausgewählt werden. Dieses ist auf die Anforderungen an den jeweiligen Cloud-Dienst abzustimmen.

Bei der Nutzung von Cloud-Diensten werden die festgelegten Sicherheitsanforderungen integraler Bestandteil der Beschaffungsverträge oder Vereinbarungen mit der Dienstleister*in.

Der gesamte Auswahl- und Beschaffungsprozess ist detailliert zu dokumentieren, um Transparenz und Nachvollziehbarkeit sicherzustellen. Dies umfasst die genauen Kriterien, die Wirtschaftlichkeitsbetrachtung, die Auswahl des Lizenz- oder Tarifmodells und die Aufnahme der Sicherheitsanforderungen in Verträge.

3.5 Test und Freigabe

Vor der Produktivnutzung der Cloud-Services sind folgende Vorgaben zu beachten:

Vor der Produktivnutzung müssen Funktionstests durch den Cloud-Owner durchgeführt werden. Hierfür ist ein detaillierter Testplan zu erstellen, um die Leistungsfähigkeit und Zuverlässigkeit der Cloud-Services zu überprüfen.

Die Einhaltung der Sicherheitsanforderungen sind vor der Produktivnutzung durch den Cloud-Owner auf Umsetzung und Wirksamkeit zu testen. Etwaige Schwachstellen werden identifiziert und behoben, um eine sichere Nutzung zu gewährleisten. Hierzu gehört insbesondere die Prüfung, ob das geplante Rollen- und Rechtemanagement in der Cloud umsetzbar ist.

Die Freigabe der Cloud-Services erfolgt in Abstimmung mit dem Informationssicherheits-Management und anderen relevanten Stakeholdern. Dies schließt die Datenschutzbeauftragte und bei Bedarf den Betriebsrat bei mitbestimmungspflichtigen Angelegenheiten ein.

Alle durchgeführten Tests und die Freigabe sind umfassend zu dokumentieren. Die Dokumentation beinhaltet Testergebnisse, vorgenommene Anpassungen und die Zustimmung der interessierten Parteien. Die Dokumentation dient der Nachvollziehbarkeit und Transparenz des Test- und Freigabeprozesses.

3.6 Einsatz und laufender Betrieb

Der laufende Betrieb des Cloud-Dienstes erfordert eine präzise Regelung von Support und Zuständigkeiten zwischen dem Goethe-Institut, insbesondere im Bereich des Fachbereichs, der IT-Infrastruktur, und dem Cloud-Anbieter. Die festgelegten Regelungen müssen nicht nur definiert, sondern auch konsequent umgesetzt werden, um einen reibungslosen Ablauf sicherzustellen.

Im Rahmen des Änderungsmanagements wird, das erreichte Sicherheitsniveau sowohl anlassbezogen als auch regelmäßig durch den Cloud-Owner überprüft und bewertet. Hierbei liegt der Fokus auf der kontinuierlichen Anpassung an sich verändernde Bedrohungen und Anforderungen. Dieser Prozess gewährleistet eine stetige Optimierung der Sicherheitsmaßnahmen.

Die regelmäßige Kontrolle der Leistungserbringung und Abrechnung stellt sicher, dass der Cloud-Anbieter die vereinbarten Service Level Agreements (SLAs) einhält. Etwaige Ausfallzeiten oder eine verringerte Verfügbarkeit werden dabei überprüft und daraufhin bewertet, ob diese durch die festgelegten SLAs abgedeckt sind.

Die Überprüfung der Zertifizierung oder des Sicherheitsnachweises des Cloud-Anbieters ist ein entscheidender Schritt, um sicherzustellen, dass die Sicherheitsstandards weiterhin den Anforderungen entsprechen. Diese Überprüfung erfolgt in regelmäßigen Abständen durch den Cloud-Owner, um eine fortwährende Vertrauenswürdigkeit des Dienstleisters zu gewährleisten.

Es muss sichergestellt werden, dass in der Cloud nur die gemäß der Planung abgestimmten Informationen verarbeitet werden. Diese Kontrolle ist essenziell, um Datenschutzrichtlinien und Compliance-Anforderungen zu erfüllen.

Die Einhaltung der mit der Anbieter*in abgestimmten Prozesse ist zu überwachen und es muss darauf geachtet werden, dass die Kontaktdaten aktuell sind. Dies stellt sicher, dass die Zusammenarbeit reibungslos verläuft und etwaige Anpassungen oder Mitteilungen zeitnah kommuniziert werden können.

3.7 Beendigung und Außerbetriebnahme

Damit eine Außerbetriebnahme eines Cloud-Services möglich ist sind folgende Vorgaben zu beachten und bereits bei der Beschaffung zu berücksichtigen.

Vor der Außerbetriebnahme ist ein detaillierter Plan für die Datenmigration zu erstellen. Dieser Plan definiert den zeitlichen Ablauf, die Auswahl der zu migrierenden Informationen und die Zielumgebung. Die Abstimmung mit dem Cloud-Anbieter ist im Vorfeld durchzuführen, um etwaige technische Herausforderungen zu identifizieren und zu bewältigen.

Die vollständige Löschung aller Daten bei der Cloud-Anbieter*in ist sicherzustellen. Die Verantwortlichkeiten für diesen Prozess sind klar zwischen der Organisation und der Cloud-Anbieter*in zu definieren, um den Datenschutzrichtlinien gerecht zu werden.

Es ist eine Übergangsfrist zwischen der Entscheidung zur Außerbetriebnahme und der Umsetzung zu vereinbaren. Diese Frist ermöglicht einen reibungslosen Übergang, in dem alle Schritte, einschließlich der Datenmigration und Löschung, sorgfältig durchgeführt werden können. Etwaige Rückfragen oder zusätzliche Klärungen können in dieser Zeit ebenfalls erfolgen.

Der gesamte Prozess der Außerbetriebnahme ist sorgfältig zu dokumentieren. Dies beinhaltet den Migrationsplan, die Löschung der Informationen bei der Cloud-Anbieter*in und die Vereinbarung der Übergangsfrist. Die Dokumentation dient nicht nur der Compliance, sondern auch als Referenz für zukünftige Cloud-Nutzungen und Audits.

Die Einhaltung dieser Vorgaben ist verbindlich und gewährleistet einen sicheren und effizienten Abschluss des Cloud-Nutzungszyklus, wodurch potenzielle Risiken bei der Außerbetriebnahme von Cloud-Services minimiert werden.

4 ANLAGEN

Die folgenden Dokumente gelten in der aktuellen Version.

Nr.	Dokument
[1]	Ausführungsbestimmung Informationssicherheitskonzept
[2]	Mindeststandard des BSI zur Nutzung externer Cloud-Dienste
[3]	Kriterienkatalog Cloud Computing C5
[4]	BSI IT-Grundschutzkompendiums
[5]	Ausführungsbestimmung Kryptografie
[6]	Ausführungsbestimmung Berechtigungsmanagement
[7]	Ergänzenden Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud)

Goethe-Institut e. V.

Abteilung Zentrale Dienste

Informationssicherheit / Unternehmenssicherheit

Oskar-von-Miller-Ring 18

80333 München

Deutschland

IT-Sicherheit@goethe.de