Bundesamt
für Sicherheit in der
Informationstechnik

APP.1.1 Office-Produkte

1. Beschreibung

1.1. Einleitung

Die Gruppe der Office-Produkte umfasst in erster Linie Anwendungen, die dazu dienen, Dokumente zu erstellen, zu bearbeiten oder zu betrachten. Dazu zählen unter anderem die freie Anwendung LibreOffice und die proprietäre Anwendung Microsoft Office, die in vielen Institutionen genutzt werden. Office-Produkte gehören für die meisten Institutionen zur notwendigen IT-Grundausstattung. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen sowie Zeichenprogramme und einfache Datenbanksysteme.

1.2. Zielsetzung

Ziel des vorliegenden Bausteins ist der Schutz der Informationen, die durch Office-Produkte verarbeitet und genutzt werden. Dazu werden spezielle Anforderungen an die Funktionsweise der Komponenten von Office-Produkten gestellt. Der Baustein zeigt Anforderungen auf, die zur Absicherung von Office-Produkten vor spezifischen Gefährdungen erfüllt werden sollten.

1.3. Abgrenzung und Modellierung

Der Baustein APP.1.1 *Office-Produkte* ist auf jedes Office-Produkt anzuwenden, das lokal installiert ist und mit dem Dokumente betrachtet, bearbeitet oder erstellt werden, außer E-Mail-Anwendungen.

Dieser Baustein betrachtet den Einsatz von Office-Produkten aus Sicht des IT-Betriebs und gibt Hinweise für Benutzende, wie Office-Produkte eingesetzt werden sollten. Ergänzend zu den Anforderungen dieses Bausteins müssen die Anforderungen des übergeordneten Bausteins APP.6 *Allgemeine Software* umgesetzt werden. E-Mail-Anwendungen werden in diesem Baustein nicht berücksichtigt, die entsprechenden Anforderungen sind im Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* zu finden. Bei der Verwendung von integrierten Datenbanksystemen wie Base in LibreOffice oder Access in Microsoft Office muss der Baustein APP.4.3 *Relationale Datenbanken* berücksichtigt werden. Ebenfalls im vorliegenden Baustein ausgenommen sind reine Cloud-Office-Anwendungen wie Google Workspace mit den Anwendungen Docs oder Sheets. Anforderungen an Cloud-Anwendungen sind in dem Baustein OPS.2.2 *Cloud-Nutzung* festgelegt.

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.1.1 *Office-Produkte* von besonderer Bedeutung.

2.1. Fehlende Anpassung der Office-Produkte an den Bedarf der Institution

Werden Office-Produkte beschafft oder angepasst, ohne die Anforderungen an diese Software zu beachten, kann der Betrieb erheblich gestört werden. Es kann beispielsweise sein, dass vorhandene Vorlagen und Dokumente nicht kompatibel sind oder mit Anwendungen von Geschäftspartnern und -partnerinnen nicht interoperabel ist. Sollten Office-Produkte nicht an den Bedarf der Institution angepasst werden, kann dies zu Performance-Verlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

2.2. Schädliche Inhalte in Office-Dokumenten

Office-Dokumente können in der Regel verschiedene sogenannte „Aktive Inhalte“ oder Makros enthalten, die mitunter für komplexe Automatisierungen genutzt werden. Aktive Inhalte können aber auch Schadcode enthalten, der ausgeführt wird, wenn das Dokument geöffnet wird. Solche Schadfunktionen in Office-Dokumenten können die betroffenen Dokumente selbst, aber auch andere Daten und Programme manipulieren. Darüber hinaus kann sich der Schadcode weiter ausbreiten. Alle betroffenen Geschäftsprozesse der Institution können in ihren Funktionen gestört oder blockiert werden. Im schlimmsten Fall bleibt die Manipulation unerkannt und führt zu Sicherheitslücken und zur Verarbeitung von verfälschten Informationen.

2.3. Integritätsverlust von Office-Dokumenten

Die Integrität von Office-Dokumenten kann verfälscht werden, wenn unbeabsichtigt oder vorsätzlich die Inhalte geändert werden. Durch einen unbedachten Umgang mit Office-Produkten oder durch Unkenntnis der Benutzenden im Umgang mit Office-Dokumenten können Dokumente unerkannt geändert werden. Dies ist dann besonders problematisch, wenn es sich um produktiv eingesetzte Dokumente handelt. Wird mit Dokumenten weitergearbeitet, die unerkannt verfälscht wurden, werden möglicherweise falsche Entscheidungen getroffen oder es kann ein Image-Schaden für die Institution entstehen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.1 *Office-Produkte* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der oder die ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

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	Benutzende

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.1.1.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.1.A2 Einschränken von Aktiven Inhalten (B)

Die Funktion, dass eingebettete Aktive Inhalte automatisch ausgeführt werden, MUSS deaktiviert werden. Falls es dennoch notwendig ist, Aktive Inhalte auszuführen, MUSS darauf geachtet werden, dass Aktive Inhalte nur ausgeführt werden, wenn sie aus vertrauenswürdigen Quellen stammen. Alle Benutzenden MÜSSEN hinsichtlich der Funktionen, die Aktive Inhalte einschränken, eingewiesen werden.

APP.1.1.A3 Sicheres Öffnen von Dokumenten aus externen Quellen (B) [Benutzende]

Alle aus externen Quellen bezogenen Dokumente MÜSSEN auf Schadsoftware überprüft werden, bevor sie geöffnet werden. Alle als problematisch eingestuften und alle innerhalb der Institution nicht benötigten Dateiformate MÜSSEN verboten werden. Falls möglich, SOLLTEN sie blockiert werden. Durch technische Maßnahmen SOLLTE erzwungen werden, dass Dokumente aus externen Quellen geprüft werden.

APP.1.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.1.A17 Sensibilisierung zu spezifischen Office-Eigenschaften (B)

Alle Benutzenden MÜSSEN geeignet bezüglich der Gefährdungen durch Aktive Inhalte in Office-Dateien sensibilisiert werden. Die Benutzenden MÜSSEN zum Umgang mit Dokumenten aus externen Quellen geeignet sensibilisiert werden.

Die Benutzenden SOLLTEN über die Möglichkeiten und Grenzen von Sicherheitsfunktionen der eingesetzten Software und der genutzten Speicherformate informiert werden. Den Benutzenden SOLLTE vermittelt werden, mit welchen Funktionen sie Dokumente vor nachträglicher Veränderung und Bearbeitung schützen können.

Benutzende SOLLTEN im Umgang mit den Verschlüsselungsfunktionen in Office-Produkten sensibilisiert 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.1.1.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.1.A6 Testen neuer Versionen von Office-Produkten (S)

Neue Versionen von Office-Produkten SOLLTEN vor dem produktiven Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln wie Makros, Dokumentenvorlagen oder Formularen der Institution geprüft werden (Siehe hierzu OPS.1.1.6 *Software-Tests und -Freigaben).* Es SOLLTE sichergestellt sein, dass

wichtige Arbeitsmittel auch mit der neuen Software-Version einwandfrei funktionieren. Bei entdeckten Inkompatibilitäten SOLLTEN geeignete Lösungen für die betroffenen Arbeitsmittel gefunden werden.

APP.1.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.1.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.1.A10 Regelung der Software-Entwicklung durch Endbenutzende (S)

Für die Software-Entwicklung auf Basis von Office-Anwendungen, z. B. mit Makros, SOLLTEN verbindliche Regelungen getroffen werden (siehe auch APP.1.1.A2 *Einschränken von Aktiven Inhalten)*. Zunächst SOLLTE in jeder Institution die Grundsatzentscheidung getroffen werden, ob solche Eigenentwicklungen überhaupt erwünscht sind. Die Entscheidung SOLLTE in den betroffenen Sicherheitsrichtlinien dokumentiert werden. Werden Eigenentwicklungen erlaubt, SOLLTE ein Verfahren für den Umgang mit entsprechenden Funktionen der Office-Produkte für die Endbenutzenden erstellt werden. Zuständigkeiten SOLLTEN klar definiert werden. Alle notwendigen Informationen über die erstellten Anwendungen SOLLTEN angemessen dokumentiert werden. Aktuelle Versionen der Regelungen SOLLTEN allen betroffenen Benutzenden zeitnah zugänglich gemacht und von diesen beachtet werden.

APP.1.1.A11 Geregelter Einsatz von Erweiterungen für Office-Produkte (S)

Alle Erweiterungen von Office-Produkten, wie Add-ons und Extensions, SOLLTEN vor dem produktiven Einsatz genauso getestet werden wie neue Versionen. Hierbei SOLLTE ausschließlich auf isolierten Testsystemen getestet werden. Die Tests SOLLTEN prüfen, ob Erweiterungen negative Auswirkungen auf die Office-Produkte und die laufenden IT-Systeme haben. Die Tests der eingesetzten Erweiterungen SOLLTEN einem definierten Testplan folgen. Dieser Testplan SOLLTE so gestaltet sein, dass Dritte das Vorgehen nachvollziehen können.

APP.1.1.A12 Verzicht auf Cloud-Speicherung (S) [Benutzende]

Die in einigen Office-Produkten integrierten Funktionen für Cloud-Speicher SOLLTEN grundsätzlich deaktiviert werden. Alle Cloud-Laufwerke SOLLTEN deaktiviert werden. Alle Dokumente SOLLTEN durch die Benutzenden auf zentral verwalteten Fileservern der Institution gespeichert werden. Um Dokumente für Dritte freizugeben, SOLLTEN spezialisierte Anwendungen eingesetzt werden. Diese Anwendungen SOLLTEN mindestens über eine verschlüsselte Datenablage und -versendung sowie ein geeignetes System zur Konten- und Rechteverwaltung verfügen.

APP.1.1.A13 Verwendung von Viewer-Funktionen (S) [Benutzende]

Daten aus potenziell unsicheren Quellen SOLLTEN automatisch in einem geschützten Modus geöffnet werden. Diese Funktion SOLLTE NICHT durch die Benutzenden deaktivierbar sein. Eine Liste vertrauenswürdiger Quellen SOLLTE definiert werden, von denen Inhalte unmittelbar geöffnet und bearbeitet werden können.

In dem geschützten Modus SOLLTEN Daten NICHT unmittelbar bearbeitet werden können. Aktive Inhalte, wie Makros und Skripte, SOLLTEN im geschützten Modus NICHT automatisch ausgeführt werden. Nur eine allgemeine Navigation SOLLTE ermöglicht werden. Wenn die Dokumente lediglich betrachtet werden sollen, SOLLTEN entsprechende Viewer-Anwendungen verwendet werden, wenn diese verfügbar sind.

APP.1.1.A14 Schutz gegen nachträgliche Veränderungen von Dokumenten (S) [Benutzende]

Je nach geplantem Verwendungszweck von Dokumenten SOLLTEN Dokumente geeignet gegen nachträgliche Veränderung geschützt werden.

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.1.1.A15 Einsatz von Verschlüsselung und Digitalen Signaturen (H)

Daten mit erhöhtem Schutzbedarf SOLLTEN nur verschlüsselt gespeichert bzw. übertragen werden. Bevor ein in ein Office-Produkt integriertes Verschlüsselungsverfahren genutzt wird, SOLLTE geprüft werden, ob es einen ausreichenden Schutz bietet. Zusätzlich SOLLTE ein Verfahren eingesetzt werden, mit dem Makros und Dokumente digital signiert werden können.

APP.1.1.A16 Integritätsprüfung von Dokumenten (H)

Wenn Daten mit erhöhtem Schutzbedarf gespeichert oder übertragen werden, SOLLTEN geeignete Verfahren zur Integritätsprüfung eingesetzt werden. Falls Daten vor Manipulation geschützt werden sollen, SOLLTEN darüber hinaus kryptografische Verfahren eingesetzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat in den „BSI-Veröffentlichungen zur Cyber-Sicherheit“ folgende Dokumente zur sicheren Konfiguration von Office Produkten veröffentlicht:

- BSI-CS 135: Sichere Konfiguration von Microsoft Office 2013/2016/2019
- BSI-CS 136: Sichere Konfiguration von Microsoft Excel 2013/2016/2019
- BSI-CS 137: Sichere Konfiguration von Microsoft PowerPoint 2013/2016/2019
- BSI-CS 138: Sichere Konfiguration von Microsoft Word 2013/2016/2019
- BSI-CS 139: Sichere Konfiguration von Microsoft Outlook 2013/2016/2019
- BSI-CS 140: Sichere Konfiguration von Microsoft Access 2013/2016/2019
- BSI-CS 141: Sichere Konfiguration von Microsoft Visio 2013/2016/2019
- BSI-CS 146: Sichere Konfiguration von Libre Office - Empfehlungen für Unternehmen mit einer verwalteten Umgebung
- BSI-CS 147: Sichere Konfiguration von Libre Office - Empfehlungen für Privatanwender und Privatanwenderinnen, kleine Unternehmen

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A, A.9.4 System and application access control & A.12.5 Control of operational Software Vorgaben, die auf den Betrieb von Office-Produkten zutreffen.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.1.2 Webbrowser

1. Beschreibung

1.1. Einleitung

Webbrowser sind Anwendungsprogramme, die (Hypertext-) Dokumente, Bilder, Video-, Audio- und andere Datenformate aus dem Internet abrufen, verarbeiten, darstellen, ausgeben und auf lokalen IT-Systemen speichern können. Ebenso können Webbrowser auch Daten ins Internet übertragen.

Stationäre und mobile Clients sind heute ohne Webbrowser nicht vorstellbar, weil sehr viele private und geschäftliche Anwendungen entsprechende Inhalte nutzen. Gleichzeitig werden diese Inhalte im Internet immer vielfältiger. Die meisten Webseiten nutzen eingebettete Videos, animierte Elemente und andere aktive Inhalte. Moderne Webbrowser decken zudem eine große Bandbreite an Zusatzfunktionen ab, indem sie Plug-ins und externe Bibliotheken einbinden. Hinzu kommen Erweiterungen für bestimmte Funktionen, Datenformate und Inhalte. Die Komplexität moderner Webbrowser bietet ein hohes Potenzial für gravierende konzeptionelle Fehler und programmtechnische Schwachstellen. Sie erhöht nicht nur die möglichen Gefahren für Angriffe aus dem Internet, sondern birgt zusätzliche Risiken durch Programmier- und Bedienungsfehler.

Die Risiken für die Vertraulichkeit und Integrität von Daten sind erheblich. Ebenso ist die Verfügbarkeit des gesamten IT-Systems durch solche Schwachstellen bedroht. Internetinhalte müssen demzufolge aus Sicht des Webbrowsers grundsätzlich als nicht vertrauenswürdig angesehen werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Sicherheitsanforderungen für Webbrowser, die auf Clients, also auf stationären und mobilen IT-Systemen sowie auch auf Tablets und Smartphones, eingesetzt werden, zu beschreiben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.1.2 *Webbrowser* ist auf jeden Webbrowser einmal anzuwenden.

Er enthält grundsätzliche Sicherheitsanforderungen, die bei der Installation und dem Betrieb von Webbrowsern für den Zugriff auf Daten aus dem Internet zu beachten und zu erfüllen sind.

Webbrowser sind eine der am häufigsten genutzten Anwendungen. Sie greifen auf ungeprüfte, potentiell schädliche Daten im Internet zu und stellen damit ein Einfallstor für Angriffe dar, oft mit dem Ziel, sich weiter auf das Betriebssystem auszubreiten. Um die Betriebssysteme abzusichern, sollten

daher die Anforderungen der Bausteine der Schichten SYS.2 *Desktop-Systeme* und SYS.3.2 *Tablet und Smartphone* erfüllt werden.

Mit Browsern genutzte Webanwendungen sowie zuständige Server werden in den Bausteinen APP.3.1 *Webanwendungen und Webservices* und APP.3.2 *Webserver* behandelt.

Allgemeine Anforderungen an den sicheren Einsatz von Software sind in diesem Baustein nicht enthalten. Sie sind im Baustein APP.6 *Allgemeine Software* zu finden, der zusätzlich zu diesem Baustein anzuwenden ist.

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.1.2 *Webbrowser* von besonderer Bedeutung.

2.1. Ausführung von Schadcode durch Webbrowser

Webbrowser laden regelmäßig Daten aus nicht vertrauenswürdigen Quellen. Solche Daten können ausführbaren Schadcode enthalten, der Schwachstellen ausnutzen kann und das IT-System der Benutzenden ohne deren Kenntnis infiziert.

Dabei kann es sich um Code handeln, der durch den Webbrowser direkt ausgeführt werden kann, wie etwa JavaScript oder WebAssembly. Ebenso kann es auch ausführbarer Code eines Plug-ins oder einer Erweiterung im Kontext des Browsers sein, wie etwa Java oder Bestandteile von PDF-Dokumenten. Schließlich kann es sich auch um Code handeln, der vom Webbrowser auf den Client geladen und dort außerhalb des Browser-Prozesses ausgeführt wird. Werden die grundlegenden Schutzmechanismen moderner Webbrowser nicht ausreichend angewendet, werden die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Diensten des Clients oder möglicherweise sogar der mit ihm verbundenen Netze bedroht.

2.2. Exploit Kits

Schwachstellenlisten und sogenannte Exploit Kits erleichtern die Entwicklung individueller Schadsoftware erheblich. Cyberangriffe können automatisiert werden, um Drive-by-Downloads oder andere Verbreitungswege leicht und ohne Expertenwissen zu nutzen. Angreifende können ihnen bekannte Schwachstellen der Webbrowser, der verbundenen Ressourcen oder Erweiterungen ausnutzen, um Folgeangriffe vorzubereiten oder Code mit Schadfunktion auf den Clients zu laden und zu installieren. Oft wird durch den so auf den Clients geladenen Schadcode weitere Schadsoftware nachgeladen, die dann auf den Clients mit den Rechten der Benutzenden ausgeführt wird.

2.3. Mitlesen der Internetkommunikation

Die grundlegende Sicherheit der Kommunikation im Internet hängt wesentlich vom eingesetzten Authentisierungsverfahren und von der Verschlüsselung der Daten auf dem Transportweg ab.

Fehlerhafte Implementierungen der entsprechenden Verfahren sind möglich und verhindern eine wirkungsvolle Authentisierung und Verschlüsselung. Viele Webdienste bieten außerdem immer noch veraltete Verschlüsselungsverfahren an. Somit kann bei einem Angriff die Authentisierung von Servern unterlaufen werden oder die Kommunikation bzw. die Daten werden nicht wirkungsvoll verschlüsselt. Hierdurch können Informationen auf dem Übertragungsweg mitgelesen oder verändert werden. In der Vergangenheit wurden außerdem Zertifizierungsstellen kompromittiert. Angreifende könnten so an Zertifikate für fremde Websites gelangen.

2.4. Integritätsverlust in Webbrowsern

Werden Webbrowser, Plug-ins oder Erweiterungen aus nicht vertrauenswürdigen Quellen bezogen, können unabsichtlich und unbemerkt Schadfunktionen ausgeführt werden. Angreifende können beispielsweise Browserkomponenten wie Toolbars fälschen, um die Benutzenden auf manipulierte Kopien von Webseiten zu locken, mit deren Hilfe Phishing-Angriffe durchgeführt werden. Bösartige Erweiterungen können Inhalte der betrachteten Webseiten manipulieren oder Daten ausspionieren und an die Angreifenden senden.

2.5. Verlust der Privatsphäre

Werden Webbrowser unsicher konfiguriert, können vertrauenswürdige Daten zufällig oder böswillig unbefugten Dritten zugänglich gemacht werden. Auch Passwörter können ungewollt weitergegeben werden. Werden Cookies, Passwörter, Historien, Eingabedaten und Suchanfragen gespeichert oder unnötige Erweiterungen aktiviert, können Daten von Dritten oder von Schadprogrammen leichter missbräuchlich ausgelesen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.2 *Webbrowser* 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	Benutzende

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.1.2.A1 Verwendung von grundlegenden Sicherheitsmechanismen (B)

Der eingesetzte Webbrowser MUSS sicherstellen, dass jede Instanz und jeder Verarbeitungsprozess nur auf die eigenen Ressourcen zugreifen kann (Sandboxing). Webseiten MÜSSEN als eigenständige Prozesse oder mindestens als eigene Threads voneinander isoliert werden. Plug-ins und Erweiterungen MÜSSEN ebenfalls in isolierten Bereichen ausgeführt werden.

Der verwendete Webbrowser MUSS die Content Security Policy (CSP) umsetzen. Der aktuell höchste Level der CSP SOLLTE erfüllt werden.

Der Browser MUSS Maßnahmen zur Same-Origin-Policy und Subresource Integrity unterstützen.

APP.1.2.A2 Unterstützung sicherer Verschlüsselung der Kommunikation (B)

Der Webbrowser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Verbindungen zu Webservern MÜSSEN mit TLS verschlüsselt werden, falls dies vom Webserver unterstützt wird. Unsichere Versionen von TLS SOLLTEN deaktiviert werden. Der Webbrowser MUSS

den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen und einsetzen.

APP.1.2.A3 Verwendung von vertrauenswürdigen Zertifikaten (B)

Falls der Webbrowser eine eigene Liste von vertrauenswürdigen Wurzelzertifikaten bereitstellt, MUSS sichergestellt werden, dass nur der IT-Betrieb diese ändern kann. Falls dies nicht durch technische Maßnahmen möglich ist, MUSS den Benutzenden verboten werden, diese Liste zu ändern. Außerdem MUSS sichergestellt werden, dass der Webbrowser Zertifikate lokal widerrufen kann.

Der Webbrowser MUSS die Gültigkeit der Server-Zertifikate mithilfe des öffentlichen Schlüssels und unter Berücksichtigung des Gültigkeitszeitraums vollständig prüfen. Auch der Sperrstatus der Server-Zertifikate MUSS vom Webbrowser geprüft werden. Die Zertifikatskette einschließlich des Wurzelzertifikats MUSS verifiziert werden.

Der Webbrowser MUSS den Benutzenden eindeutig und gut sichtbar darstellen, ob die Kommunikation im Klartext oder verschlüsselt erfolgt. Der Webbrowser SOLLTE den Benutzenden auf Anforderung das verwendete Serverzertifikat anzeigen können. Der Webbrowser MUSS den Benutzenden signalisieren, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Der Webbrowser MUSS in diesem Fall die Verbindung abbrechen, bis die Benutzenden diese ausdrücklich bestätigt haben.

APP.1.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.2.A6 Kennwortmanagement im Webbrowser (B)

Wird ein Kennwortmanager im Webbrowser verwendet, MUSS er eine direkte und eindeutige Beziehung zwischen Webseite und hierfür gespeichertem Kennwort herstellen. Der Kennwortspeicher MUSS die Passwörter verschlüsselt speichern. Es MUSS sichergestellt werden, dass auf die im Kennwortmanager gespeicherten Passwörter nur nach Eingabe eines Master-Kennworts zugegriffen werden kann. Außerdem MUSS sichergestellt sein, dass die Authentisierung für den kennwortgeschützten Zugriff nur für die aktuelle Sitzung gültig ist.

Der IT-Betrieb MUSS sicherstellen, dass der verwendete Browser den Benutzenden die Möglichkeit bietet, gespeicherte Passwörter zu löschen.

APP.1.2.A13 Nutzung von DNS-over-HTTPS (B)

Die Institution MUSS entscheiden, ob die verwendeten Browser DNS-over-HTTPS (DoH) verwenden sollen. Die Browser MÜSSEN entsprechend dieser Entscheidung konfiguriert werden.

Falls ein interner DNS-Resolver verwendet wird, MUSS dieser auch vom Browser 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.1.2.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.2.A7 Datensparsamkeit in Webbrowsern (S) [Benutzende]

Cookies von fremden Institutionen SOLLTEN im Webbrowser abgelehnt werden. Gespeicherte Cookies SOLLTEN durch die Benutzenden gelöscht werden können.

Die Funktion zur Autovervollständigung von Daten SOLLTE deaktiviert werden. Wird die Funktion dennoch genutzt, SOLLTEN die Benutzenden diese Daten löschen können. Die Benutzenden SOLLTE außerdem die Historiendaten des Webbrowsers löschen können.

Sofern vorhanden, SOLLTE eine Synchronisation des Webbrowsers mit Cloud-Diensten deaktiviert werden. Telemetriefunktionen sowie das automatische Senden von Absturzberichten, URL-Eingaben und Sucheingaben aus der Institution heraus oder an Externe SOLLTEN soweit wie möglich deaktiviert werden.

Peripheriegeräte wie Mikrofon oder Webcam sowie Standortfreigaben SOLLTEN nur für Webseiten aktiviert werden, bei denen sie unbedingt benötigt werden. Der Browser SOLLTE eine Möglichkeit bieten, WebRTC, HSTS und JavaScript zu konfigurieren bzw. abzuschalten.

APP.1.2.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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.1.2.A9 Einsatz einer isolierten Webbrowser-Umgebung (H)

Die Institution SOLLTE speziell abgesicherte, isolierte Browserumgebungen einsetzen, wie z. B. ReCoBS oder virtualisierte Instanzen.

APP.1.2.A10 Verwendung des privaten Modus (H) [Benutzende]

Der Webbrowser SOLLTE bei erhöhten Anforderungen bezüglich der Vertraulichkeit im sogenannten privaten Modus ausgeführt werden, sodass keine Informationen oder Inhalte dauerhaft auf dem IT-System der Benutzenden gespeichert werden. Der Browser SOLLTE so konfiguriert werden, dass lokale Inhalte beim Beenden gelöscht werden.

APP.1.2.A11 Überprüfung auf schädliche Inhalte (H)

Aufgerufene Internetadressen SOLLTEN durch den Webbrowser auf potenziell schädliche Inhalte geprüft werden. Der Webbrowser SOLLTE die Benutzenden warnen, wenn Informationen über schädliche Inhalte vorliegen. Eine als schädlich klassifizierte Verbindung SOLLTE NICHT aufgerufen werden können. Das verwendete Verfahren zur Überprüfung DARF NICHT gegen Datenschutz- oder Geheimschutz-Vorgaben verstoßen.

APP.1.2.A12 Zwei-Browser-Strategie (H)

Für den Fall von ungelösten Sicherheitsproblemen mit dem verwendeten Webbrowser SOLLTE ein alternativer Browser mit einer anderen Plattform installiert sein, der den Benutzenden als Ausweichmöglichkeit dient.

4. Weiterführende Informationen

4.1. Wissenswertes

- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 047: „Absicherungsmöglichkeiten beim Einsatz von Webbrowsern“
- Mindeststandard des BSI für den Einsatz des SSL/ TLS-Protokoll durch Bundesbehörden nach § 8 Abs. 1 Satz 1 BSIG
- Mindeststandard des BSI für Webbrowser nach § 8 Absatz 1 Satz 1 BSIG
- Common Criteria Protection Profile for Remote-Controlled Browsers Systems (ReCoBS): BSI-PP-0040

Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.1.4 Mobile Anwendungen (Apps)

1. Beschreibung

1.1. Einleitung

Smartphones, Tablets und ähnliche mobile Geräte sind heute auch in Behörden und Unternehmen weit verbreitet. Mitarbeitende können so unabhängig von Ort und Zeit auf Daten der Institution, auf Informationen und Anwendungen zugreifen.

Mobile Anwendungen (Applikationen, kurz Apps) sind Anwendungen, die auf mobil genutzten Betriebssystemen wie iOS oder Android auf entsprechenden Endgeräten installiert und ausgeführt werden. Apps werden üblicherweise aus sogenannten App Stores bezogen. Diese werden oft von den herstellenden Institutionen der mobil genutzten Betriebssysteme und Endgeräte betrieben und gepflegt. Im professionellen Umfeld ist es aber auch üblich, Apps selbst zu entwickeln und z. B. über Mobile-Device-Management-Lösungen (MDM) auf den Endgeräten zu installieren und zu verwalten. Im Vergleich zu Anwendungen auf Desktop-Betriebssystemen unterliegen Apps unter iOS oder Android besonderen Rahmenbedingungen, wie etwa einem durch das Betriebssystem sichergestellten Berechtigungsmanagement.

Für die unterschiedlichen mobilen Betriebssysteme gibt es mittlerweile eine große Auswahl an verfügbaren Apps. Auch gibt es standardisierte Bibliotheken und Entwicklungsumgebungen, mit deren Hilfe sich Apps im Vergleich zu klassischen Anwendungen schnell selbst entwickeln lassen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die auf mobilen Endgeräten mit Apps verarbeitet werden. Auch die Einbindung von Apps in eine bestehende IT-Infrastruktur wird dabei betrachtet. Der Baustein definiert zudem Anforderungen, um Apps richtig auszuwählen und sicher betreiben zu können. Dabei werden die Apps unabhängig von ihrer Quelle (App Store oder eigene Installation) betrachtet.

1.3. Abgrenzung und Modellierung

Der Baustein APP.1.4 *Mobile Anwendungen (Apps)* ist auf alle Anwendungen anzuwenden, die auf mobilen Endgeräten eingesetzt werden.

Der Baustein betrachtet Apps unter mobilen Betriebssystemen wie iOS und Android. Anforderungen, welche die zugrundeliegenden Betriebssysteme betreffen, werden hier nicht berücksichtigt. Diese Anforderungen finden sich beispielsweise in den Bausteinen SYS.3.2.3 *iOS (for Enterprise)* sowie SYS.3.2.4 *Android*. Oft werden Apps zentral über ein Mobile Device Management verwaltet. Anforderungen hierzu können dem Baustein SYS.3.2.2 *Mobile Device Management (MDM)* entnommen werden.

Ebenso sind anwendungsspezifische Aspekte von Apps nicht Gegenstand des Bausteins zu mobilen Anwendungen. Diese werden in den entsprechenden Bausteinen der Schicht APP *Anwendungen, wie z. B.* APP.1.2 *Webbrowser* behandelt.

Apps greifen häufig auf Backend-Systeme oder Server bzw. Anwendungsdienste zurück. Werden die Backend-Systeme oder Server selber betrieben, werden Sicherheitsempfehlungen dazu nicht an dieser Stelle gegeben, sondern in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums. Dazu gehören beispielsweise APP.3.1 *Webanwendungen und Webservices* oder APP.4.3 *Relationale Datenbanken*. Zusätzlich sollten die Bausteine berücksichtigt werden, die sich mit allgemeinen Aspekten von Anwendungen befassen, etwa OPS.1.1.6 *Software-Tests und -Freigaben* oder APP.6 *Allgemeine Software*, da diese Aspekte nicht im vorliegenden Baustein berücksichtigt werden. Bei der Entwicklung eigener Apps sollten die Anforderungen des Bausteins CON.8 *Software-Entwicklung* berücksichtigt werden.

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.1.4 *Mobile Anwendungen (Apps)* von besonderer Bedeutung.

2.1. Ungeeignete Auswahl von Apps

Die ausgewählten Apps wirken sich stark auf die damit verarbeiteten Informationen, auf das mobile Endgerät sowie häufig auf die IT-Infrastruktur der Institution aus. Wird dies bei der Auswahl der Apps nicht berücksichtigt, können weitreichende Probleme entstehen. Besonders hoch ist die Gefahr, wenn es sich dabei um Apps handelt, die nicht eigens für die abzubildenden Geschäftsprozesse entwickelt wurden. So könnten beispielsweise die für den Betrieb einer App erforderlichen Voraussetzungen nicht ausreichend betrachtet werden. Möglicherweise ist dann z. B. die mobile Netzanbindung nicht leistungsfähig genug oder die Hardware nicht kompatibel. Apps können auch dann ungeeignet sein, wenn sie keine ausreichende langfristige Einsatzstabilität und -planung bieten oder von den herstellenden Institutionen nicht ausreichend gepflegt werden.

2.2. Zu weitreichende Berechtigungen

Apps benötigen gewisse Berechtigungen, um auf bestimmte Funktionen und Dienste zugreifen zu können. So kann eine App in der Regel immer auf die Internetverbindung des mobilen Endgeräts zugreifen. Der Standort oder das Adressbuch müssen hingegen meist gesondert freigegeben werden. Werden Apps eingesetzt, die zu weitgehende Berechtigungen erfordern, oder werden die Berechtigungen nicht ausreichend eingeschränkt, so kann sich das insbesondere auf die Vertraulichkeit und Integrität der Informationen auf dem Endgerät auswirken. Apps können zudem Informationen an unberechtigte Dritte weitergeben, wie z. B. den Standort, Fotos oder Kontakt- und Kalenderdaten. Außerdem sind Apps in der Lage, lokal abgespeicherte Daten zu verändern oder zu löschen. Schließlich können Apps auch Kosten verursachen, etwa durch Telefonanrufe, versendete SMS oder In-App-Käufe.

2.3. Ungewollte Funktionen in Apps

Zwar prüfen manche App-Store-Betreibende die angebotenen Apps, dennoch können diese Sicherheitslücken oder bewusst eingesetzte Schadfunktionen enthalten. Das Risiko ist insbesondere dann hoch, wenn Apps aus ungeprüften oder unzuverlässigen Quellen bezogen werden. Dann kann die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen gefährdet werden.

2.4. Software-Schwachstellen und Fehler in Apps

Apps können Schwachstellen enthalten, über die sie direkt am Gerät oder über Netzverbindungen angegriffen werden können. Außerdem werden viele Apps nach einiger Zeit von den Entwickelnden nicht mehr weiter gepflegt. Dadurch werden erkannte Sicherheitsmängel nicht mehr durch entsprechende Updates behoben.

2.5. Unsichere Speicherung lokaler Anwendungsdaten

Einige Apps speichern Daten auf dem Endgerät, beispielsweise Profile der Benutzenden oder Dokumente. Falls diese Daten unzureichend geschützt sind, können möglicherweise andere Apps darauf zugreifen. Dies betrifft neben bewusst abgelegten Daten auch temporäre Daten, wie beispielsweise im Cache zwischengespeicherte Informationen. Auch sind sie für Unberechtigte leicht lesbar, z. B. wenn Mitarbeitende ihre Geräte verloren haben. Außerdem werden lokal gespeicherte Informationen oft nicht im Datensicherungskonzept berücksichtigt. Fällt das Endgerät aus oder geht verloren, sind die lokal gespeicherten Informationen ebenfalls nicht mehr verfügbar.

2.6. Ableitung vertraulicher Informationen aus Metadaten

Durch Apps sammeln sich viele Metadaten an. Mithilfe dieser Metadaten können Dritte auf vertrauliche Informationen schließen, z. B. über Telefon- und Netzverbindungen, Bewegungsdaten oder besuchte Webseiten. Daraus lassen sich dann weitere Informationen ableiten, beispielsweise die Organisationsstruktur der Institution, genaue Positionen von Standorten sowie deren personelle Besetzung.

2.7. Abfluss von vertraulichen Daten

Daten werden über verschiedene Wege von und zu einer App übertragen. Dafür stellen mobile Betriebssysteme verschiedene Schnittstellen bereit. Benutzende haben ebenfalls verschiedene Möglichkeiten, Daten mit einer App auszutauschen, etwa lokal über eine Speicherkarte, die Zwischenablage, die Gerätekamera oder andere Anwendungen. Außerdem können Daten über Cloud-Dienste oder Server der App- oder Geräte-anbietenden Institution übertragen werden. Darüber können Dritte Zugriff auf die vertraulichen Daten erlangen. Schließlich kann auch das Betriebssystem selbst Daten für den schnelleren Zugriff zwischenspeichern (Caching). Dabei können Daten versehentlich abfließen oder Angreifende auf vertrauliche Informationen zugreifen.

2.8. Unsichere Kommunikation mit Backend-Systemen

Viele Apps kommunizieren mit Backend-Systemen, über die Daten mit dem Datennetz der Institution ausgetauscht werden. Die Daten werden bei mobilen Geräten zumeist über unsichere Netze wie ein Mobilfunknetz oder WLAN-Hotspots übertragen. Werden für die Kommunikation mit Backend-Systemen aber unsichere Protokolle verwendet, können Informationen abgehört oder manipuliert werden.

2.9. Kommunikationswege außerhalb der Infrastruktur der Institution

Wenn Apps unkontrolliert mit Dritten kommunizieren können, kann dies Kommunikationswege schaffen, die nicht von der Institution erkannt und kontrolliert werden können. So können Benutzende beispielsweise die App eines Cloud-Datenspeicherdienstes nutzen, um Informationen vom Endgerät nach außen zu übertragen. Auch die enge Verzahnung von Social-Media-Diensten mit vielen Apps erschwert die Kontrolle, ob und wie Informationen das Endgerät verlassen. Diese Art von Kommunikationswegen ist nur schwer nachzuvollziehen. Dies kann noch weitere Probleme verursachen, etwa wenn Informationen oder Vorgänge archiviert werden müssen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.4 *Mobile Anwendungen (Apps)* 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

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.1.4.A1 Anforderungsanalyse für die Nutzung von Apps (B) [Fachverantwortliche]

In der Anforderungsanalyse MÜSSEN insbesondere Risiken betrachtet werden, die sich aus der mobilen Nutzung ergeben. Die Institution MUSS prüfen, ob ihre Kontroll- und Einflussmöglichkeiten auf die Betriebssystemumgebung mobiler Endgeräte ausreichend sind, um sie sicher nutzen zu können.

APP.1.4.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A5 Minimierung und Kontrolle von App-Berechtigungen (B) [Fachverantwortliche]

Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so fixiert werden, dass sie nicht durch Personen oder Apps geändert werden können. Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.

Bevor eine App in einer Institution eingeführt wird, MUSS sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen MÜSSEN hinterfragt und gegebenenfalls unterbunden werden.

APP.1.4.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A7 Sichere Speicherung lokaler App-Daten (B)

Wenn Apps auf interne Dokumente der Institution zugreifen können, MUSS sichergestellt sein, dass die lokale Datenhaltung der App angemessen abgesichert ist. Insbesondere MÜSSEN Zugriffsschlüssel verschlüsselt abgelegt werden. Außerdem DÜRFEN vertrauliche Daten NICHT vom Betriebssystem an anderen Ablageorten zwischengespeichert werden.

APP.1.4.A8 Verhinderung von Datenabfluss (B)

Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Profile über die Benutzenden erstellt werden, MUSS die App-Kommunikation geeignet eingeschränkt werden. Dazu SOLLTE die Kommunikation im Rahmen des Test- und Freigabeverfahrens analysiert werden. Weiterhin SOLLTE überprüft werden, ob eine App ungewollte Protokollierungs- oder Hilfsdateien schreibt, die möglicherweise vertrauliche Informationen enthalten.

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.1.4.A3 Verteilung schutzbedürftiger Apps (S)

Interne Apps der Institution und Apps, die schutzbedürftige Informationen verarbeiten, SOLLTEN über einen institutionseigenen App Store oder via MDM verteilt werden.

APP.1.4.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.4.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.4.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.4.A12 Sichere Deinstallation von Apps (S)

Werden Apps deinstalliert, SOLLTEN auch Daten gelöscht werden, die auf externen Systemen, beispielsweise bei den App-Anbietenden, gespeichert wurden.

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.1.4.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.1.4.A14 Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps (H)

Falls möglich, SOLLTE für die Authentisierung in Apps ein zweiter Faktor benutzt werden. Hierbei SOLLTE darauf geachtet werden, dass eventuell benötigte Sensoren oder Schnittstellen in allen verwendeten Geräten vorhanden sind. Zusätzlich SOLLTE bei biometrischen Verfahren berücksichtigt werden, wie resistent die Authentisierung gegen mögliche Fälschungsversuche ist.

APP.1.4.A15 Durchführung von Penetrationstests für Apps (H)

Bevor eine App für den Einsatz freigegeben wird, SOLLTE ein Penetrationstest durchgeführt werden. Dabei SOLLTEN alle Kommunikationsschnittstellen zu Backend-Systemen sowie die lokale Speicherung von Daten auf mögliche Sicherheitslücken untersucht werden. Die Penetrationstests SOLLTEN regelmäßig und zusätzlich bei größeren Änderungen an der App wiederholt werden.

APP.1.4.A16 Mobile Application Management (H)

Falls möglich, SOLLTE für das zentrale Konfigurieren von dienstlichen Apps ein Mobile Application Management verwendet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) stellt mit dem Leitfaden „Apps & Mobile Services - Tipps für Unternehmen“ (2. Auflage, 2014) eine Entscheidungshilfe zum Thema Apps und Mobile Services in Unternehmen bereit.

Das Information Security Forum (ISF) bietet eine Broschüre mit dem Titel „Securing Mobile Apps - Embracing mobile, balancing control“ (2018) an.

Auch die „NIST Special Publication 800-163: Vetting the Security of Mobile Applications“ (2015) bietet weiterführende Informationen zum Thema Apps.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.1 Allgemeiner Verzeichnisdienst

1. Beschreibung

1.1. Einleitung

Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. In einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel können zu einer Kennung der Name und Vorname des oder der Benutzenden, die Personalnummer und der Name des IT-Systems abgelegt werden. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen und Zertifikate für elektronische Signaturen
- Benutzendenverwaltung, z. B. zur Verwaltung von Konten und Berechtigungen
- Bereitstellung eines Backend-Dienstes für Authentifizierungsfunktionen, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise vorwiegend abgerufen werden. Schreibzugriffe, bei denen Einträge erstellt, geändert oder gelöscht werden, sind seltener notwendig.

Wenn ein Verzeichnisdienst eingesetzt wird, können manche Verwaltungsaufgaben innerhalb des Netzes, wie z. B. Kontenerstellung, Passwortänderungen und Zuweisungen von Rollen und Gruppen, an zentraler Stelle durchgeführt werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, allgemeine Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* ist für alle verwendeten Verzeichnisdienste anzuwenden.

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Verzeichnisdiensten unabhängig vom eingesetzten Produkt. Für produktspezifische Sicherheitsaspekte gibt es im IT-Grundschutz-Kompendium weitere Bausteine, die zusätzlich auf den jeweiligen Verzeichnisdienst anzuwenden sind. Bausteine zu Server-Betriebssystemen, auf denen Verzeichnisdienste üblicherweise betrieben werden, sind in der Schicht SYS.1 *Server* des IT-Grundschutz-Kompendiums aufgeführt. Grundlegende Anforderungen an Software-Produkte finden sich in APP.6 *Allgemeine Software* und sind ebenfalls zu beachten.

Verzeichnisdienste sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung,* OPS.1.2.5 *Fernwartung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mitberücksichtigt werden.

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.2.1 *Allgemeiner Verzeichnisdienst* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

Die Sicherheit von Verzeichnisdiensten stützt sich stark auf die Sicherheit des Basisbetriebssystems und dabei vor allem auf die Dateisystemsicherheit. Verzeichnisdienste lassen sich auf vielen Betriebssystemen installieren und betreiben, wodurch sich eine große Vielfalt der vorzunehmenden Sicherheitseinstellungen ergeben kann. Diese Vielfalt erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse über das jeweilige Betriebssystem voraus. Sollte die entstehende Gesamtlösung sehr heterogen oder komplex sein, kann ein nicht ausreichend geplanter Einsatz des Verzeichnisdienstes im Wirkbetrieb zu Sicherheitslücken führen.

2.2. Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

Durch eine Partitionierung können die Verzeichnisdaten eines Verzeichnisdienstes in einzelne Teilbereiche (Partitionen) aufgeteilt werden. Um für eine bessere Lastverteilung zu sorgen, werden Partitionen des Verzeichnisdienstes häufig auf weitere Instanzen repliziert. Außerdem wird durch die redundante Datenhaltung die Ausfallsicherheit verbessert und somit die Verfügbarkeit erhöht. Von entscheidender Bedeutung ist deshalb auch hier eine geeignete Planung, da Partitions- und Replikationseinstellungen zwar nachträglich geändert werden können, dies aber Probleme verursachen kann. Es kann etwa zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Ausfällen führen.

2.3. Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die durchzuführenden Aufgaben

erforderlich sind. Dies gilt auch für die Berechtigungen, die über einen Verzeichnisdienst verwaltete Benutzende und Gruppen erhalten, auch wenn diese für die Informationen *im* Verzeichnisdienst selbst gelten. Werden diese Rechte fehlerhaft administriert, kann einerseits der Betrieb gestört werden, falls erforderliche Rechte nicht zugewiesen wurden. Andererseits können Sicherheitslücken entstehen, falls über die notwendigen Rechte hinaus weitere Rechte vergeben werden. Wenn die Zugriffsrechte im Verzeichnisdienst falsch oder inkonsistent vergeben werden, ist dadurch die Sicherheit des Gesamtsystems erheblich gefährdet. Ein besonders kritischer Punkt sind auch die Administrationsrechte. Werden diese Rechte falsch vergeben, kann das gesamte Administrationskonzept unterlaufen oder unter Umständen sogar die Administration des Verzeichnissystems selbst verhindert oder eine unberechtigte Nutzung ermöglicht werden.

2.4. Fehlerhafte Konfiguration des Zugriffs auf Verzeichnisdienste

In vielen Fällen müssen weitere Applikationen wie Internet- oder Intranet-Anwendungen auf den Verzeichnisdienst zugreifen. Eine Fehlkonfiguration kann dazu führen, dass Zugriffsrechte falsch vergeben werden. Es kann auch passieren, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann oder dass Daten zur Authentisierung im Klartext übermittelt werden. In diesem Fall können Informationen während der Übertragung ausgespäht werden.

2.5. Ausfall von Verzeichnisdiensten

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen können Verzeichnisdienste oder Teile davon ausfallen. Als Folge sind die Daten im Verzeichnis temporär nicht mehr zugänglich. Im Extremfall können auch Daten verloren gehen oder Anmeldungen an vom Verzeichnisdienst bedienten IT-Systemen nicht mehr möglich sein. Dadurch können Geschäftsprozesse und interne Arbeitsabläufe behindert werden. Sind funktionsfähige Kopien der ausgefallenen Systemteile vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch je nach gewählter Netztopologie nur mit eingeschränkter Leistungsfähigkeit.

2.6. Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff

Wenn es Angreifenden gelungen ist, eine notwendige Authentisierung gegenüber dem Verzeichnisdienst erfolgreich durchzuführen oder zu umgehen, können sie danach unbefugt auf eine Vielzahl von Daten zugreifen. Somit kann potentiell der gesamte Verzeichnisdienst kompromittiert werden. Dadurch könnte das gesamte betroffene System beeinträchtigt oder gar zerstört werden.

Die Sicherheit eines Verzeichnisdienstes kann ebenfalls gefährdet werden, wenn anonyme Benutzende zugelassen werden. Dadurch, dass deren Identität nicht überprüft wird, können anonyme Benutzende zunächst beliebige Abfragen an den Verzeichnisdienst richten, durch die sie zumindest Teilinformationen über dessen Struktur und Inhalt erlangen. Wenn anonyme Zugriffe zugelassen werden, sind außerdem DoS-Attacken auf den Verzeichnisdienst leichter durchzuführen, da Angreifende mehr Zugriffsmöglichkeiten haben, die nur schlecht kontrollierbar sind.

2.7. Fehlerhafte Konfiguration von Verzeichnisdiensten

Verzeichnisdienste verfügen über zahlreiche Funktionen, sodass der Verzeichnisdienst von Anwendenden mit sehr unterschiedlichen Bedürfnissen genutzt werden kann. Eine Fehlkonfiguration dieser zahlreichen Funktionen kann dazu führen, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann. Wenn beispielsweise die Standardkonfiguration nicht ausreichend geprüft und angepasst wird, können die Informationen zur Authentisierung im Klartext oder unzureichend abgesichert übermittelt und damit ausgespäht werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.1 *Allgemeiner Verzeichnisdienst* 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, Datenschutzbeauftragte

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.2.1.A1 Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste (B)

Es MUSS eine Sicherheitsrichtlinie für den Verzeichnisdienst erstellt werden. Diese SOLLTE mit dem übergreifenden Sicherheitskonzept der gesamten Institution abgestimmt sein.

APP.2.1.A2 Planung des Einsatzes von Verzeichnisdiensten (B) [Datenschutzbeauftragte, Fachverantwortliche]

Der Einsatz von Verzeichnisdiensten MUSS sorgfältig geplant werden. Die konkrete Nutzung des Verzeichnisdienstes MUSS festgelegt werden. Es MUSS sichergestellt sein, dass der Verzeichnisdienst und alle ihn verwendenden Anwendungen kompatibel sind. Zudem MUSS ein Konzept für eine Struktur aus Objektklassen und Attributtypen entwickelt werden, dass den Ansprüchen der vorgesehenen Nutzungsarten genügt. Bei der Planung eines Verzeichnisdienstes, der personenbezogene Daten beinhaltet, MÜSSEN Personalvertretung und Datenschutzbeauftragte beteiligt werden. Es MUSS ein bedarfsgerechtes Berechtigungskonzept zum Verzeichnisdienst entworfen werden. Generell SOLLTE die geplante Verzeichnisdienststruktur vollständig dokumentiert und die Dokumentation bei Änderungen fortgeschrieben werden. Maßnahmen SOLLTEN geplant und umgesetzt werden, die es unterbinden, aus dem Verzeichnisdienst unbefugt Daten sammeln zu können.

APP.2.1.A3 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste (B) [Fachverantwortliche]

Die Administration des Verzeichnisdienstes selbst und die eigentliche Verwaltung der Daten MÜSSEN getrennt werden. Alle administrativen Aufgabenbereiche und Berechtigungen SOLLTEN ausreichend dokumentiert werden.

Bei einer eventuellen Zusammenführung mehrerer Verzeichnisdienstbäume MÜSSEN die daraus resultierenden effektiven Rechte kontrolliert werden.

APP.2.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.1.A5 Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten (B)

Der Verzeichnisdienst MUSS sicher konfiguriert werden. Für die sichere Konfiguration einer Verzeichnisdienste-Infrastruktur MÜSSEN neben dem Server auch die Clients (IT-Systeme und Anwendungen) einbezogen werden.

Wird die Konfiguration des Verzeichnisdienstes oder der mit ihm vernetzten IT-Systeme geändert, SOLLTEN die Benutzenden rechtzeitig über Wartungsarbeiten informiert werden.

APP.2.1.A6 Sicherer Betrieb von Verzeichnisdiensten (B)

Die Sicherheit des Verzeichnisdienstes MUSS im Betrieb permanent aufrechterhalten werden. Alle den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse SOLLTEN nachvollziehbar dokumentiert und aktuell gehalten werden. Sofern der Verzeichnisdienst zur Verwaltung von Anmeldedaten verwendet wird, MÜSSEN dedizierte Clients bei der Fernwartung eingesetzt werden. Der Zugriff auf alle Administrationswerkzeuge MUSS für normale Benutzende unterbunden werden.

APP.2.1.A17 Absicherung von schutzbedürftigen Anmeldeinformationen (B)

Für Attribute, die schutzbedürftige Anmeldeinformationen wie beispielsweise Passwörter enthalten, MUSS der Zugriff stark eingeschränkt 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.2.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A8 Planung einer Partitionierung im Verzeichnisdienst (S)

Sofern eine Partitionierung geplant ist, SOLLTE sich diese an den Schutzzielen des Verzeichnisdienstes orientieren und diese geeignet unterstützen. Eine Partitionierung SOLLTE so geplant werden, dass sie die Schadensauswirkungen bei Sicherheitsvorfällen begrenzt, die unabhängige Administration verschiedener Partitionen ermöglicht und organisatorischen bzw. Sicherheitsgrenzen folgt.

APP.2.1.A9 Geeignete Auswahl von Komponenten für Verzeichnisdienste (S) [Fachverantwortliche]

Für den Einsatz eines Verzeichnisdienstes SOLLTEN geeignete Komponenten identifiziert werden. Es SOLLTE unter Berücksichtigung von APP.6 *Allgemeine Software* ein Anforderungskatalog erstellt werden, nach dem die Komponenten für den Verzeichnisdienst ausgewählt und beschafft werden. Im Rahmen der Planung und Konzeption des Verzeichnisdienstes SOLLTEN passend zum Einsatzzweck Anforderungen an dessen Sicherheit formuliert werden. Insbesondere SOLLTE bereits bei der Produktauswahl berücksichtigt werden, wie weitere Sicherheitsanforderungen unter Einsatz der jeweiligen Komponente umgesetzt werden können.

APP.2.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A11 Einrichtung des Zugriffs auf Verzeichnisdienste (S)

Der Zugriff auf den Verzeichnisdienst SOLLTE entsprechend der Sicherheitsrichtlinie konfiguriert werden. Wird der Verzeichnisdienst als Server im Internet eingesetzt, SOLLTE er entsprechend durch ein Sicherheitsgateway geschützt werden.

APP.2.1.A12 Überwachung von Verzeichnisdiensten (S)

Verzeichnisdienste SOLLTEN gemeinsam mit dem Server beobachtet und protokolliert werden, auf dem sie betrieben werden. Insbesondere Änderungen innerhalb des Verzeichnisdienstes sowie Konfigurationsänderungen des Verzeichnisdienstes SOLLTEN vorrangig protokolliert werden.

APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten (S)

Werden vertrauliche Informationen übertragen, SOLLTE die gesamte Kommunikation mit dem Verzeichnisdienst über ein sicheres Protokoll entsprechend der Technischen Richtlinie TR-02102 des BSI (z. B. TLS) verschlüsselt werden. Der Datenaustausch zwischen Client und Verzeichnisdienst-Server SOLLTE abgesichert werden. Es SOLLTE definiert werden, auf welche Daten zugegriffen werden darf.

APP.2.1.A14 Geregelte Außerbetriebnahme eines Verzeichnisdienstes (S) [Fachverantwortliche]

Bei einer Außerbetriebnahme des Verzeichnisdienstes SOLLTE sichergestellt sein, dass weiterhin benötigte Rechte bzw. Informationen in ausreichendem Umfang zur Verfügung stehen. Alle anderen Rechte und Informationen SOLLTEN gelöscht werden. Zudem SOLLTEN die Benutzenden darüber informiert werden, wenn ein Verzeichnisdienst außer Betrieb genommen wird. Bei der Außerbetriebnahme einzelner Partitionen eines Verzeichnisdienstes SOLLTE darauf geachtet werden, dass dadurch andere Partitionen nicht beeinträchtigt werden.

APP.2.1.A15 Migration von Verzeichnisdiensten (S)

Bei einer geplanten Migration von Verzeichnisdiensten SOLLTE vorab ein Migrationskonzept erstellt werden. In dem Migrationskonzept SOLLTE berücksichtigt werden, ob das Berechtigungsmanagement von altem und neuem Verzeichnisdienst analog funktioniert oder ob neue Berechtigungsstrukturen erforderlich sind. Die Schema-Änderungen, die am Verzeichnisdienst vorgenommen wurden, SOLLTEN vor der Migration analysiert und dokumentiert werden. Weitreichende Berechtigungen, die dazu verwendet wurden, die Migration des Verzeichnisdienstes durchzuführen, SOLLTEN wieder zurückgesetzt werden. Bei der Migration SOLLTE berücksichtigt werden, dass IT-Systeme, die auf den Verzeichnisdienst zugreifen, gegebenenfalls lokale Caches vorhalten oder aus anderen Gründen dort eine Aktualisierung der migrierten Verzeichnisdienstinhalte initiiert werden muss.

APP.2.1.A18 Planung einer Replikation im Verzeichnisdienst (S)

Bei jeder Replikation MUSS festgelegt werden, welches Ziel diese Replikation verfolgt. Dafür SOLLTEN eine Replikationstopologie und -strategie gewählt werden, die zum Ziel bzw. Einsatzszenario passen. Bei Replikationen, die nicht der Hochverfügbarkeit des Dienstes dienen, MUSS der replizierte Inhalt des Verzeichnisdienstes auf die erforderlichen Objekte beschränkt werden. Um die Replikationen zeitgerecht ausführen zu können, SOLLTE eine ausreichende Bandbreite sichergestellt werden.

APP.2.1.A19 Umgang mit anonymen Zugriffen auf Verzeichnisdienste (S)

Sollen anonymen Benutzenden auf einzelne Teilbereiche des Verzeichnisbaums Zugriffe eingeräumt werden, so SOLLTE hierfür ein Proxy-Dienst vorgelagert werden. Dieser Proxy-Dienst SOLLTE über ein gesondertes Konto, einen sogenannten Proxy-User, auf den eigentlichen Verzeichnisdienst zugreifen. Die Zugriffsrechte für diesen Proxy-User SOLLTEN hinreichend restriktiv vergeben werden. Sie SOLLTEN zudem wieder komplett entzogen werden, wenn der Account nicht mehr gebraucht wird. Damit nicht versehentlich schutzbedürftige Informationen herausgegeben werden, SOLLTE die Suchfunktion des Verzeichnisdienstes dem Einsatzzweck angemessen eingeschränkt werden.

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.2.1.A16 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes (H)

Im Rahmen der Notfallvorsorge SOLLTE es eine bedarfsgerechte Notfallplanung für Verzeichnisdienste geben. Für den Ausfall wichtiger Verzeichnisdienst-Systeme SOLLTEN Notfallpläne vorliegen. Alle Notfall-Prozeduren für die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten SOLLTEN dokumentiert werden.

APP.2.1.A20 Absicherung der Replikation (H)

Replikationen von vertraulichen Inhalten SOLLTEN zusätzlich zu einer Verschlüsselung auf Applikations- oder Transportebene durch z. B. IPsec gesichert werden. Für die Authentisierung im Rahmen der Replikation SOLLTEN möglichst starke Authentisierungsverfahren verwendet werden.

APP.2.1.A21 Hochverfügbarkeit des Verzeichnisdienstes (H)

Es SOLLTE eine geeignete Strategie zur Hochverfügbarkeit gewählt werden. Hierbei SOLLTE entschieden werden, ob eine Master-Master-Replikation oder Master-Replica-Replikation (früher als Master-Slave-Replikation bezeichnet) geeigneter ist. Es SOLLTEN auch Randbedingungen wie verteilte Standorte oder Verhalten bei Inkonsistenzen berücksichtigt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.2 Active Directory Domain Services

1. Beschreibung

1.1. Einleitung

Active Directory (AD) ist ein Sammelbegriff für verschiedene von Microsoft für Windows Server entwickelte Serverrollen. Die Serverrolle Active Directory Domain Services (AD DS) aggregiert sowohl Funktionalitäten eines Verzeichnis-, als auch Authentifizierungs- und Autorisierungsdienstes sowie einer zentralen Konfigurationsverwaltung für Windows-Infrastrukturen.

Active Directory Domain Services wird hauptsächlich in Netzen eingesetzt, die vorrangig von Microsoft-basierten Betriebssystemen geprägt sind. Ein AD DS speichert und verwaltet Informationen zu Netzressourcen (z. B. Benutzende, Computer und Geräte). Bei Bedarf können diese Informationen, wie in LDAP-Verzeichnisdiensten üblich, auch um anwendungsspezifische Daten erweitert werden. Es dient Anwendenden und Administrierenden dazu, diese Informationen in einer hierarchischen Struktur zu organisieren, bereitzustellen und zu nutzen. Dabei strukturiert AD DS die Objekte in Namensräumen, die als Gesamtstrukturen, Domänen und Organisationseinheiten bezeichnet werden. Eine Gesamtstruktur bildet eine hierarchische Sammlung von Domänen, die jeweils mehrere Organisationseinheiten enthalten können. Die erste und damit in der Hierarchie oben angeordnete Domäne, die in einer Gesamtstruktur angelegt wird, übernimmt systembedingt die Rolle der „Gesamtstruktur Stammdomäne“ (englisch „forest root domain“) und beinhaltet die administrativen Gruppen, die für gesamtstrukturweite Verwaltungsaufgaben wie beispielsweise das Hinzufügen weiterer Domänen oder Schemaänderungen zuständig sind. Alle Domänen innerhalb einer Gesamtstruktur sind implizit durch bidirektionale, transitive Vertrauensstellungen miteinander verknüpft, so dass die Gesamtstruktur eine logische Sicherheitsgrenze darstellt.

Als Authentisierungsprotokoll nutzt AD DS im Standard Kerberos v5 (in einer durch Microsoft erweiterten Implementierung). Zusätzlich steht weiterhin auch noch das Protokoll NTLM (New Technology LAN Manager) zur Verfügung. NTLM kann dabei einfacher von Angreifenden ausgenutzt werden. Windows Server mit der Serverrolle AD DS werden als Domänencontroller bezeichnet. Aus Verfügbarkeitsgründen werden häufig mehrere Domänencontroller verteilt eingesetzt. Das AD DS bietet außerdem die Möglichkeit eines „Read-Only-Betriebs“ eines Domänencontrollers, der für Standorte mit erhöhtem Risiko für die physische Sicherheit vorgesehen ist.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es, Active Directory Domain Services im Regelbetrieb einer Institution abzusichern, die AD DS zur Verwaltung von Windows-Systemen (Client und Server) sowie zur zentralen Authentifizierung und Autorisierung einsetzt.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.2 *Active Directory Domain Services* ist für alle verwendeten Verzeichnisdienste anzuwenden, die auf Microsoft Active Directory Domain Services basieren. Er kann zusätzlich für die Modellierung von Active Directory Lightweight Directory Services (AD LDS), die einen reduzierten Funktionsumfang von AD DS bieten, in Teilen verwendet werden.

In diesem Baustein werden die für Active Directory Domain Services spezifischen Gefährdungen und Anforderungen betrachtet. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten finden sich im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst*. Die dort beschriebenen allgemeinen Anforderungen werden im vorliegenden Baustein konkretisiert und ergänzt. Dieser Baustein wiederholt nicht die Anforderungen zur Absicherung der Betriebssysteme der Server und Clients, die für den Betrieb und die Verwaltung des AD DS genutzt werden, wie z. B. SYS.1.2.3 *Windows Server* oder SYS.2.2.3 *Clients unter Windows*. Dieser Baustein geht auch nicht erneut auf die Anforderungen der zugrundeliegenden Netzinfrastruktur ein.

Active Directory Domain Services sollte nicht losgelöst von den Bausteinen ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement,* CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung,* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration,* OPS.1.2.5 *Fernwartung*, DER.1 *Detektion von sicherheitsrelevanten Ereignissen,* DER.2 *Security Incident Management,* DER.4 *Notfallmanagement* und APP.3.6 *DNS-Server* modelliert werden. Es ist davon auszugehen, dass sich die Anforderungen dieser Bausteine wechselseitig beeinflussen.

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.2.2 *Active Directory Domain Services* von besonderer Bedeutung.

2.1. Unzureichende Planung der Sicherheitsgrenzen

In AD DS existieren verschiedene Arten von Grenzen. Diese Grenzen definieren die Gesamtstruktur (englisch Forest), die Domäne, die Standorttopologie und die Zuweisung von Rechten. Eine AD-DS-Instanz erzeugt zunächst eine Gesamtstruktur (engl. Forest) als Container auf höchster Ebene für alle Domänen dieser Instanz. Eine Gesamtstruktur kann ein oder mehrere Domänen-Containerobjekte enthalten, die über eine gemeinsame logische Struktur, einen Global Catalog, ein Schema und automatische bidirektionale, transitive Vertrauensbeziehungen verfügen. Dies bedeutet, dass zwischen Domänen innerhalb einer Gesamtstruktur sowohl das Vertrauen zueinander, also auch der Zugriff aufeinander, beidseitig möglich ist. Die Gesamtstruktur stellt also systembedingt die Sicherheitsgrenze dar, innerhalb derer Informationen standardmäßig im AD DS weitergegeben werden. Eine Domäne bildet dabei nur eine Verwaltungsgrenze. Werden Sicherheitsgrenzen nicht entlang der Gesamtstrukturgrenzen realisiert, kann eine Kompromittierung ein höheres Schadensausmaß als erwartet erzeugen, da sie zu einer Kompromittierung aller IT-Systeme in der Gesamtstruktur führen kann. Diese Gefährdung ist eine Besonderheit beim AD DS, da sich die Planung einer Partitionierung im Verzeichnisdienst produktbedingt nicht vollständig umsetzen lässt. Eine vollständige Kompromittierung einer Gesamtstruktur bedeutet, dass Angreifende Kontrolle über alle Objekte, die

zu den enthaltenen Domänen gehören, also unter anderem alle Konten und alle IT-Systeme, haben. Damit haben diese potentiell auch Kontrolle über die zugehörigen IT-Systeme und Dienste.

2.2. Zu viele oder nachlässige Vertrauensbeziehungen

Vertrauensbeziehungen zwischen Domänen und zwischen Gesamtstrukturen ermöglichen es, Konten einer anderen Domäne oder Gesamtstruktur Zugriff auf Ressourcen innerhalb der eigenen Domäne oder Gesamtstruktur zu gewähren. Werden die Vertrauensbeziehungen zwischen Gesamtstrukturen und zwischen Domänen nicht initial und regelmäßig daraufhin evaluiert, ob sie benötigt werden und ob die Sicherheitskontrollen rund um diese Vertrauensbeziehungen ausreichend sind, können Probleme mit Berechtigungen auftreten und Informationen abfließen. Insbesondere wenn die standardmäßig aktive SID-(Security Identifier)-Filterung deaktiviert wird, können komplexe, schwer zu durchschauende Konfigurationsfehler, die zu einer missbräuchlich Nutzung der Vertrauensstellung und zu weitreichenden Zugriffsrechten führen können, auftreten. Gleiches gilt, wenn auf „Selective Authentication“ bei Vertrauensbeziehungen zwischen Gesamtstrukturen verzichtet wird.

2.3. Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domänen- und Gesamtstruktur-Funktionsebenen

Bis einschließlich Windows Server 2016 bringt jede neue Generation des Betriebssystems Windows Server zusätzliche Sicherheitsfunktionen und -erweiterungen in Bezug auf AD DS in Form von Domänen- bzw. Gesamtstruktur-Funktionsebenen mit. Werden ältere Betriebssysteme als Domänencontroller bzw. veraltete Domänen- oder Gesamtstruktur-Funktionsebenen eingesetzt, können zeitgemäße Sicherheitsfunktionen nicht genutzt werden. Dies erhöht die Gefahr unsicherer Standardeinstellungen. Eine unsicher konfigurierte Gesamtstruktur oder Domäne gefährdet die darin verarbeiteten Informationen und erleichtert Angriffe durch Dritte.

2.4. Betrieb weiterer Rollen und Dienste auf Domänencontrollern

Werden neben AD DS auf einem Domänencontroller noch weitere Dienste betrieben, erhöht dies, neben den durch AD DS sowieso schon stark kumulierten Diensten, zusätzlich die Angriffsfläche dieser zentralen Komponente durch mögliche zusätzliche Schwachstellen und Fehlkonfigurationen. Solche Dienste können bewusst oder unbewusst missbraucht werden, um z. B. Informationen unberechtigt zu kopieren, zu verändern oder, im Fall von Schwachstellen oder Fehlkonfigurationen, die zur Kompromittierung des Domänencontrollers führen, die Domäne oder Gesamtstruktur zu übernehmen.

2.5. Unzureichende Überwachung und Dokumentation von delegierten Rechten

Wenn die Bildung unternehmensspezifischer Gruppen und die Delegation von Rechten an diese Gruppen- oder an einzelne Benutzendenobjekte nicht systematisch geplant und umgesetzt wird, kann die Delegation nur noch schwer kontrolliert werden. Sie könnte dann etwa viel mehr Zugriffe einräumen als vorgesehen, was durch Dritte missbraucht werden kann. Eine fehlende regelmäßige Auditierung der Zugriffsrechte von Gruppen- und einzelnen Benutzendenobjekte kann das Problem zusätzlich verschärfen. Auch wenn Standardgruppen genutzt und ihre Rechte an eigene Gruppen delegiert werden, etwa bei der Delegation von „Account Operators“ / „Konten-Operatoren“ an Helpdesk-Mitarbeitende, werden in der Regel mehr Rechte gewährt als tatsächlich benötigt werden.

2.6. Unsichere Authentisierung

Sogenannte „Legacy"- (also historische) Authentisierungsmechanismen im Bereich AD DS wie LAN Manager (LM) und NT LAN Manager (NTLM) v1 sind unsicher und können bei Angriffen unter bestimmten Bedingungen missbraucht werden. Angreifende können beispielsweise ohne Kenntnis der Klartextpasswörter Rechte erhalten und missbrauchen und so Teile der Domäne, die Domäne selbst oder sogar die Gesamtstruktur kompromittieren.

2.7. Zu mächtige oder schwach gesicherte Konten

Anwendungssoftware setzt manchmal Rechte hochprivilegierter Gruppen (beispielsweise von sogenannten *Domänenadministratoren*) für Dienstkonten voraus, um die Produkte einfacher testen und ausbringen zu können, obwohl für den Betrieb deutlich weniger Rechte notwendig sind. Ein besonderes Risiko besteht, wenn diese Dienstkonten mit schwachen Passwörtern gesichert sind. Auch Konten, die nicht Mitglied einer hoch privilegierten Gruppe sind, können administrative Berechtigungen beispielsweise auf einer großen Anzahl von Servern und Clients zugewiesen sein. Damit besitzen sie ähnlich umfangreiche Rechte wie Mitglieder hoch privilegierten Gruppen im AD DS. Die weitreichenden Rechte dieser Konten können von Angreifenden missbraucht werden, um sich in der Domäne weiterzubewegen.

2.8. Nutzung desselben lokalen Administrierendenpassworts auf mehreren IT-Systemen

Auch bei Domänenzugehörigkeit eines IT-Systems ist eine Anmeldung mit lokalen Konten an diesem IT-System weiterhin möglich. Werden dieselben lokalen Anmeldeinformationen auf mehreren IT-Systemen verwendet, kann eine Anmeldung mit diesen unter anderem mit dem lokalen Built-In-Konto *Administrator* auf mehreren IT-Systemen erfolgen. Dies erleichtert Angreifenden die laterale Bewegung und damit die Ausbreitung in der Infrastruktur. Damit steigt das Risiko, dass Angreifende auf einem der IT-Systeme Anmeldeinformationen eines Domänenkontos mit höheren Rechten finden und diese missbrauchen können, um die Domäne und potentiell die Gesamtstruktur zu kompromittieren.

2.9. Unsichere Speicherung von Passwörtern

Die Speicherung der Passwörter erfolgt in der zentralen AD-DS-Datenbank (*ntds.dit*) auf dem Domänencontroller produktbedingt unter anderem mittels MD4-Hashfunktion ohne Salt. Diese Hashfunktion erfüllt nicht die Anforderungen der Technischen Richtlinie TR-02102-1 „Kryptografische Verfahren: Empfehlungen und Schlüssellängen" des BSI. Unautorisierte lesende Zugriffe auf die gespeicherten Passwörter sind daher besonders kritisch. Aufgrund der weiten Verbreitung von AD DS existieren viele Werkzeuge, um die Hashes der Passwörter zu extrahieren. Die AD-DS-Datenbank kann beispielsweise unter Verwendung weiterer auf dem Domänencontroller hinterlegter Schlüssel offline entschlüsselt werden und den Zugriff auf die Hashes ermöglichen. Zudem ist durch die schwache Hashfunktion ein Ermitteln der Klartextpasswörter möglich.

2.10. Unzureichende Absicherung von Domänencontrollern

Jeder (Read-Write)-Domänencontroller einer Domäne hält ein vollständiges Replikat der zentralen AD-DS-Datenbank (*ntds.dit*) vor, in der die Passwörter unsicher gespeichert sind. Neben dem unzureichenden Schutz vor Zugriff durch Dritte auf die Domänencontroller im Betrieb kann auch ein ungeeignetes Backupverfahren zum Abgreifen der zentralen AD-DS-Datenbank und in Folge zum Abfluss von Informationen und der Kompromittierung der Domäne und potentiell der Gesamtstruktur führen. Auch der Betrieb von virtualisierten Domänencontrollern gemeinsam mit weniger schützenswerten virtuellen Maschinen auf einem physischen Virtualisierungshost kann zu

einer Kompromittierung des AD DS führen. Dies gilt auch, wenn die administrativen Konten des Virtualisierungshosts, die durch ihre administrativen Tätigkeiten Vollzugriff auf AD DS besitzen, nicht angemessen geschützt werden.

2.11. Hinterlassen von hochprivilegierten Anmeldeinformationen auf Domänenmitgliedsservern und -clients

Erfolgt eine Anmeldung oder Dienstnutzung mit hochprivilegierten Konten auf einem Server oder Client der Domäne, so werden die zugehörigen Anmeldeinformationen auf diesem zwischengespeichert (z. B. im Speicher des Local Security Authority Subsystem / LSASS). Im Fall einer Kompromittierung können Angreifende diese dort extrahieren. Dadurch kann die Kompromittierung eines einzelnen Servers oder Clients der Domäne dazu führen, dass die gesamte Domäne und potentiell die Gesamtstruktur kompromittiert wird.

2.12. Hinzufügen nicht vertrauenswürdiger IT-Systemen zur Windows-Domäne

In den voreingestellten Konfigurationen dürfen alle im AD DS authentifizierten Benutzenden bis zu zehn IT-Systeme zu der Domäne hinzufügen, auch, wenn sie keine administrativen Berechtigungen im AD DS besitzen. Dadurch können sie IT-Systeme in die Domäne hinzufügen, auf denen sie hohe Privilegien besitzen. Diese Privilegien können als Ausgangspunkt für weitere Angriffe verwendet werden. Da das Hinzufügen von IT-Systemen zu einer Domäne eine Verwaltungsaufgabe ist, die typischerweise in einen IT-Prozess eingebettet ist, können hier schwer vorhersehbare Seiteneffekt entstehen, wenn IT-Systeme unkontrolliert der Domäne beitreten, ohne diesen Prozess korrekt zu durchlaufen.

2.13. Vermaschung von administrativen Privilegien durch Integration von weiteren Anwendungen

Werden Anwendungen mit einer Integration in AD DS eingesetzt (beispielsweise Microsoft Exchange), können den durch diese Anwendungen angelegten AD-DS-Konten administrative Berechtigungen in AD DS zugewiesen sein. Dadurch können Sicherheitslücken in diesen Anwendungen dazu führen, dass Angreifende weitreichende Administrationsrechte bei IT-Systemen innerhalb der Gesamtstruktur erhalten. Ein Beispiel hierfür ist die Sicherheitslücke CVE-2019-0686 (PrivExchange) in Microsoft Exchange.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.2 *Active Directory Domain Services* 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

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.2.2.A1 Planung von Active Directory Domain Services (B) [Fachverantwortliche]

Es MUSS eine Funktionsebene für die Domäne(n) und die Gesamtstruktur von mindestens Windows Server 2016 gewählt werden. Ein bedarfsgerechtes Berechtigungskonzept für die Domäne(n) und die Gesamtstruktur MUSS entworfen werden. Dabei MUSS berücksichtigt werden, dass zwischen den einzelnen Domänen einer Gesamtstruktur produktbedingt keine Sicherheitsgrenzen bestehen und daher keine sichere Begrenzung der administrativen Bereiche innerhalb einer Gesamtstruktur möglich ist. Administrative Delegationen MÜSSEN mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet sein. Die geplante Struktur einschließlich etwaiger Schema-Änderungen MUSS nachvollziehbar dokumentiert sein.

APP.2.2.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows (B)

Es MUSS ein Konzept zur Einrichtung von Gruppenrichtlinien vorliegen. Mehrfachüberdeckungen MÜSSEN beim Gruppenrichtlinienkonzept möglichst vermieden werden. In der Dokumentation des Gruppenrichtlinienkonzepts MÜSSEN Ausnahmeregelungen erkannt werden können. Alle Gruppenrichtlinienobjekte MÜSSEN durch restriktive Zugriffsrechte geschützt sein. Für die Parameter in allen Gruppenrichtlinienobjekten MÜSSEN sichere Vorgaben festgelegt sein.

APP.2.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.2.A5 Absicherung des Domänencontrollers (B)

Aufgrund der zentralen Rolle und der Schadensauswirkung bei Kompromittierung des AD DS für die Infrastruktur SOLLTE eine Risikobetrachtung durchgeführt werden. Der Notfallzugriff auf den Domänencontroller mit dem lokalen Restore-Konto DSRM (Directory Services Restore Mode) MUSS im Rahmen des Notfallmanagements geplant werden.

Auf dem Domänencontroller MUSS eine ausreichende Größe für das Sicherheitsprotokoll auf Grundlage des in DER.1 *Detektion von sicherheitsrelevanten Ereignissen* festgelegten Zeitraums eingestellt sein. Aufgrund der zentralen Bedeutung des Domänencontrollers SOLLTEN auf diesem Server keine weiteren Dienste betrieben werden, sofern diese nicht zwingend auf dem *gleichen* Server zum Betrieb des AD DS erforderlich sind.

APP.2.2.A6 Sichere Konfiguration von Vertrauensbeziehungen (B)

Alle Vertrauensbeziehungen zwischen Domänen und zwischen Gesamtstrukturen MÜSSEN regelmäßig auf ihre Notwendigkeit und Absicherungsmaßnahmen evaluiert werden. Dabei MUSS geprüft werden, ob eine bidirektionale Vertrauensbeziehung notwendig ist. Wenn eine Domäne keine bidirektionale Vertrauensbeziehung zu anderen Domänen in der Gesamtstruktur benötigt, SOLLTE diese Domäne in eine eigene Gesamtstruktur ausgelagert werden, da innerhalb einer Gesamtstruktur produktbedingt keine Anpassung der Vertrauensbeziehungen möglich ist.

Die SID-(Security Identifier)-Filterung bei Vertrauensstellungen zwischen Gesamtstrukturen DARF NICHT deaktiviert werden. Die voreingestellten SIDs DÜRFEN NICHT entfernt werden. Hat der in der Gesamtstruktur abgebildete Informationsverbund, dem vertraut wird, kein ausreichendes

Sicherheitsniveau, MUSS für die Vertrauensbeziehung zu dieser Gesamtstruktur „Selective Authentication“ verwendet werden.

APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory (B) [Fachverantwortliche]

Es MUSS sichergestellt sein, dass die Konten von Dienste-Administrierenden ausschließlich von Mitgliedern der Gruppe der Dienste-Administrierenden verwaltet werden. Bevor Konten vordefinierten AD-DS-Gruppen hinzugefügt werden, SOLLTE geprüft werden, ob alle der Gruppe zugehörigen Rechte für die mit den Konten verbundenen Tätigkeiten erforderlich sind. Den Gruppen „Schema-Admins“ / „Schema-Administratoren“ sowie der Gruppe „Enterprise Admins“ / „Organisations-Administratoren“ und „Domain Admins“ / „Domänen-Administratoren“ SOLLTEN neben dem AD-DS-Built-In-Konto für Administrierende weitere administrative Konten nur temporär für den Zeitraum zugewiesen werden, in dem sie diese Berechtigungen benötigen.

APP.2.2.A16 Härtung der AD-DS-Konten (B)

Built-in-AD-DS-Konten MÜSSEN mit komplexen Passwörtern versehen werden. Sie DÜRFEN NUR als Notfallkonten dienen. Das Built-in „Guest“- / „Gast“-Konto MUSS deaktiviert werden. Die Berechtigungen für die Gruppe „Everyone“ / „Jeder“ MUSS beschränkt werden. Privilegierte Konten MÜSSEN Mitglied der Gruppe „Protected Users“ / „Geschütze Benutzer“ sein. Für Dienstkonten MÜSSEN (Group) Managed Service Accounts verwendet werden. Vor dem Löschen nicht mehr verwendeter Konten MUSS geprüft werden, nach welcher Aufbewahrungsfrist diese gelöscht werden können. Dabei MÜSSEN die Auswirkungen auf die Detektion und gesetzliche Aufbewahrungs- und Löschfristen berücksichtigt werden. Der Zugriff auf das AdminSDHolder-Objekt SOLLTE zum Schutz der Berechtigungen besonders geschützt sein.

APP.2.2.A17 Anmelderestriktionen für hochprivilegierte Konten der Gesamtstruktur auf Clients und Servern (B)

Die Anmeldung von hochpriviligierten Domänen- und Gesamtstruktur-Konten und Gruppen MUSS technisch auf die minimal notwendigen IT-Systeme einschränkt werden. Insbesondere die Anmeldung von Mitgliedern der Gruppen „Schema Admins“ / „Schema-Administratoren“, „Enterprise Admins“ / „Enterprise-Administratoren“ und „Domain Admins“ / „Domänen-Administratoren“ SOLLTE technisch auf den Domänencontroller beschränkt werden, eine Anmeldung an anderen IT-Systemen ist für diese Gruppen also zu unterbinden.

APP.2.2.A18 Einschränken des Hinzufügens neuer Computer-Objekte zur Domäne (B)

Die Berechtigung, in der Domäne neue Computer-Objekte hinzuzufügen, MUSS auf die notwendigen administrativen Konten beschränkt 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.2.2.A8 Absicherung des „Sicheren Kanals“ (S)

Der „Sichere Kanal“ SOLLTE so konfiguriert sein, dass alle übertragenen Daten immer verschlüsselt und signiert werden.

APP.2.2.A9 Schutz der Authentisierung beim Einsatz von AD DS (S)

In der Gesamtstruktur SOLLTE konsequent das Authentisierungsprotokoll Kerberos eingesetzt werden. Dabei SOLLTE für die Absicherung AES128_HMAC_SHA1 oder AES256_HMAC_SHA1 verwendet werden. Wenn aus Kompatibilitätsgründen übergangsweise NTLMv2 eingesetzt wird, SOLLTE die Migration auf Kerberos geplant und terminiert werden. Die LM-Authentisierung und NTLMv1

MÜSSEN deaktiviert sein. Der SMB-Datenverkehr MUSS signiert sein. SMBv1 MUSS deaktiviert sein. Anonyme Zugriffe auf Domänencontroller SOLLTEN unterbunden sein. LDAP-Sitzungen SOLLTEN nur signiert und mit konfiguriertem Channel Binding Token (CBT) erfolgen.

APP.2.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.2.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.2.A12 Datensicherung für Domänencontroller (S)

Aufgrund der besonderen Gefährdung der unsicher gespeicherten Passwörter SOLLTE der Zugriff auf die Backups des Domänencontrollers vergleichbar dem Zugriff auf den Domänencontroller selbst abgesichert sein.

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.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A15 Auslagerung der Administration in eine eigene Gesamtstruktur (H)

Besonders kritische IT-Systeme und Konten zur Administration der Domänen oder der Gesamtstruktur SOLLTEN in eine eigene Gesamtstruktur (häufig als „Red Forest“ bezeichnet) ausgegliedert werden, zu der von der zu verwaltenden Gesamtstruktur eine einseitige Vertrauensstellung besteht. Dies SOLLTE im Rahmen des Notfallmanagements bei der Erstellung des Notfallhandbuchs besonders berücksichtigt werden.

APP.2.2.A19 Betrieb von virtualisierten Domänencontrollern (H)

Virtualisierte Domänencontroller SOLLTEN nicht gemeinsam mit weiteren virtuell betriebenen IT-Systemen auf dem gleichen physischen Host betrieben werden. Bei der Absicherung der administrativen Konten für den Zugriff über die Virtualisierungsschicht SOLLTE berücksichtigt werden, dass diese Vollzugriffe auf den Domänencontroller haben und dieser dann vergleichbar mit dem der Gruppe „Domain Admins“ / „Domänen-Administratoren“ ist. Der Virtualisierungshost, die IT-Systeme, die am Virtualisierungsmanagement beteiligt sind sowie die Administrationskonten für die Virtualisierungsschicht SOLLTEN NICHT zur Gesamtstruktur gehören, zu der der virtualisierte Domänencontroller gehört.

APP.2.2.A20 Trennung von Organisationseinheiten (H)

Organisationseinheiten, die aus IT-Sicherheitsgründen oder sonstigen Gründen Unabhängigkeit voneinander gewährleisten müssen, SOLLTEN sich nicht in der gleichen Gesamtstruktur befinden.

APP.2.2.A21 Konfiguration eines Schichtenmodells (H)

Die Berechtigungsstruktur innerhalb der Gesamtstruktur SOLLTE in Schichten, die sich am Schutzbedarf der Konten, IT-Systeme und Anwendungen orientieren, entworfen werden. Bei dieser

Strukturierung SOLLTEN alle Konten, IT-Systeme und Anwendungen innerhalb einer Gesamtstruktur eindeutig einer Schicht zugeordnet werden können. Konten einer höheren Schicht SOLLTEN sich nicht auf Ressourcen einer niedrigeren Schicht anmelden können. Konten einer niedrigeren Schicht SOLLTEN keine Kontrollmöglichkeit über Konten und Ressourcen höherer Schichten besitzen.

APP.2.2.A22 Zeitlich befristete Berechtigungen für die Administration (H)

Konten, die für die Administration verwendet werden, SOLLTEN nur bei Bedarf auf das benötigte Zeitfenster befristetet die für die administrative Aufgabe notwendigen Berechtigungen zugewiesen werden.

APP.2.2.A23 Regelmäßige Analyse von Berechtigungen und resultierenden Angriffspfaden (H)

Aufgrund der Komplexität von Berechtigungen, die nicht immer unmittelbar ersichtlich sind, SOLLTE eine regelmäßige Analyse der Berechtigungsstrukturen im AD DS vorgenommen werden. Insbesondere Berechtigungen, die durch die Integration von Anwendungen in AD DS entstehen (beispielsweise Microsoft Exchange) SOLLTEN kritisch auf ihre Notwendigkeit hin geprüft und auf die minimal notwendigen Berechtigungen reduziert werden. Aktualisierungen können ebenfalls auch Berechtigungsstrukturen im AD DS ändern, daher SOLLTE die Analyse auch nach entsprechenden Aktualisierungen durchgeführt werden. Mögliche Angriffspfade über die Berechtigungen der AD-DS-Konten, die beispielsweise bei Kompromittierung von Konten zur Kompromittierung der Domäne bzw. der vollständigen Gesamtstruktur führen, SOLLTEN möglichst gering sein. Die Aktivitäten der verbleibenden, als kritisch identifizierten Konten SOLLTEN besonders überwacht werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Website „Active Directory Security“ (https://adsecurity.org) enthält viele weiterführende Informationen zu AD-Sicherheit.

Der Hersteller Microsoft bietet weitergehende Informationen zu Active Directory und dessen Sicherheitsaspekten:

- Einstiegspunkt Active Directory Domain Services https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
- Dokumentation zum “Implementieren von Verwaltungsmodellen der geringsten Rechte” https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models
- Übersicht zu Domänen und Gesamtstrukturen https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)
- Sicherheitsaspekte bei Vertrauensstellungen https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)
- Dokumentation zum Schichtenmodell https://web.archive.org/web/20171205072455/https:/docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.3 OpenLDAP

1. Beschreibung

1.1. Einleitung

OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Konten, IT-Systeme oder Konfigurationen, in einer standardisierten und definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Kontenverwaltungen, aber auch Konfigurationen.

OpenLDAP stellt eine Referenz-Implementierung für einen Server-Dienst im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open-Source-Software kann OpenLDAP auf einer Vielzahl von Betriebssystemen installiert werden und gilt als einer der am meisten verbreiteten Verzeichnisdienste. Zur Besonderheit von OpenLDAP gehören die *Overlays*. Overlays erweitern den Funktionsumfang von OpenLDAP um zahlreiche Funktionen und werden auch für grundlegende Funktionen wie Protokollierung, Replikation und die Wahrung der Integrität verwendet.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, auf OpenLDAP basierende Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen geeignet zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.3 *OpenLDAP* ist auf jedes OpenLDAP-Verzeichnis anzuwenden.

In diesem Baustein werden die für OpenLDAP spezifischen Gefährdungen und Anforderungen betrachtet. Dabei wird die Version 2.4 von OpenLDAP zugrunde gelegt. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten gibt es im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst.* Diese müssen zusätzlich berücksichtigt werden. Die dort beschriebenen Anforderungen werden im vorliegenden Baustein konkretisiert und ergänzt.

OpenLDAP sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement,* CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mitberücksichtigt werden.

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.2.3 *OpenLDAP* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung von OpenLDAP

OpenLDAP kann in Verbindung mit zahlreichen anderen Anwendungen genutzt werden. Diese Anwendungen können auf die Informationen des Verzeichnisdienstes zugreifen und diese in der Regel auch ändern. Wird der Einsatz von OpenLDAP nicht oder unzureichend geplant, können folgende Probleme auftreten:

- Werden die Backends und die zugehörigen Direktiven und Parameter falsch ausgewählt, beeinflussen diese ungewollt die Funktionen, die OpenLDAP anbieten kann. Wird beispielsweise das Backend „back-ldif“ zur Datenspeicherung verwendet, um die Installation einer zusätzlichen Datenbank zu umgehen, stehen nur rudimentäre Funktionen des Verzeichnisdienstes zur Verfügung. Eine große Menge von Benutzenden oder anderen Objekten kann dann nicht geeignet verwaltet werden.
- Wenn der Einsatz von Overlays mangelhaft geplant wird, können in OpenLDAP nicht benötigte Operationen ausgeführt oder sonstige Funktionen beeinträchtigt werden. Beispielsweise werden Zugriffe auf den Verzeichnisdienst nicht oder falsch protokolliert, wenn die Debug-Funktion des slapd-Servers selbst und die Overlays „auditlog“ und „accesslog“ unzureichend geplant werden.
- OpenLDAP kann in einer ungeeigneten Systemumgebung ausgeführt werden. Wird ein verteiltes Dateisystem wie Network File System (NFS) verwendet, um die OpenLDAP-Daten abzuspeichern, könnten Dateifunktionen von OpenLDAP nicht verwendet werden. Ein Beispiel dafür ist die von vielen Datenbanken verwendete Locking-Funktion, die es ermöglicht, die Datenbank des Verzeichnisdienstes zu sperren, wenn mehrere Benutzende parallel schreibend auf die Datenbank zugreifen möchten.
- Es könnten inkompatible Versionen einer oder mehrerer Anwendungen auf die von OpenLDAP verwendeten Datenbanken zugreifen. Beispielsweise werden die Spezifikationen des Protokolls LDAPv3 nicht von OpenLDAP ohne zusätzliche Erweiterungen erfüllt. Zudem können auch Verbindungsprobleme mit den Anwendungen entstehen, wenn die falsche Version eines oder mehrerer Programme eingesetzt wird, die mit OpenLDAP nicht kompatibel sind.

2.2. Unzureichende Trennung von Offline- und Online-Zugriffen auf OpenLDAP

Auf die durch OpenLDAP verwalteten Daten (Objekte im Verzeichnisdienst ebenso wie Konfigurationseinstellungen) kann über verschiedene Möglichkeiten zugegriffen werden. Die Offline- und Online-Zugriffe erfüllen dabei ganz oder teilweise identische Funktionen. Bei einem Online-Zugriff wird über das Protokoll LDAP und den slapd auf die Daten zugegriffen. Beim Offline-Zugriff wird direkt auf die Datenbankdateien zugegriffen, bzw. es wird ein ldif-Export des Verzeichnisses editiert und anschließend wieder zurück in die Datenbank geladen. Werden diese Möglichkeiten vermischt oder wird die jeweilige Wirkungsweise vom Offline- oder Online-Zugriff fehlinterpretiert, können zahlreiche Fehler auftreten. In der Folge ist die resultierende Datenbank für OpenLDAP inkonsistent und kann somit nicht mehr fehlerfrei genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.3 *OpenLDAP* 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	Keine

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.2.3.A1 Planung und Auswahl von Backends und Overlays für OpenLDAP (B)

Der Einsatz von OpenLDAP in einer Institution MUSS sorgfältig geplant werden. Soll OpenLDAP gemeinsam mit anderen Anwendungen verwendet werden, so MÜSSEN die Planung, Konfiguration und Installation der Anwendungen mit OpenLDAP aufeinander abgestimmt werden. Für die zur Datenhaltung verwendete Datenbank MUSS sichergestellt werden, dass die verwendete Version kompatibel ist. Backends und Overlays für OpenLDAP MÜSSEN restriktiv selektiert werden. Dazu MUSS sichergestellt werden, dass die OpenLDAP-Overlays in der korrekten Reihenfolge eingesetzt werden. Bei der Planung von OpenLDAP MÜSSEN die auszuwählenden und unterstützten Client-Anwendungen berücksichtigt werden.

APP.2.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.3.A3 Sichere Konfiguration von OpenLDAP (B)

Für die sichere Konfiguration von OpenLDAP MUSS der slapd-Server korrekt konfiguriert werden. Es MÜSSEN auch die verwendeten Client-Anwendungen sicher konfiguriert werden. Bei der Konfiguration von OpenLDAP MUSS darauf geachtet werden, dass im Betriebssystem die Berechtigungen korrekt gesetzt sind. Die Vorgabewerte aller relevanten Konfigurationsdirektiven von OpenLDAP MÜSSEN geprüft und gegebenenfalls angepasst werden. Die Backends und Overlays von OpenLDAP MÜSSEN in die Konfiguration einbezogen werden. Für die Suche innerhalb von OpenLDAP MÜSSEN angemessene Zeit- und Größenbeschränkungen festgelegt werden. Die Konfiguration am slapd-Server MUSS nach jeder Änderung geprüft werden.

APP.2.3.A4 Konfiguration der durch OpenLDAP verwendeten Datenbank (B)

Die Zugriffsrechte für neu angelegte Datenbankdateien MÜSSEN auf die Kennung beschränkt werden, in deren Kontext der slapd-Server betrieben wird. Die Standard-Einstellungen der von OpenLDAP genutzten Datenbank MÜSSEN angepasst werden.

APP.2.3.A5 Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP (B)

Die in OpenLDAP geführten globalen und datenbankspezifischen Zugriffskontrolllisten (Access Control Lists) MÜSSEN beim Einsatz von OpenLDAP korrekt berücksichtigt werden. Datenbank-Direktiven MÜSSEN Vorrang vor globalen Direktiven haben.

APP.2.3.A6 Sichere Authentisierung gegenüber OpenLDAP (B)

Wenn der Verzeichnisdienst zwischen verschiedenen Benutzenden unterscheiden soll, MÜSSEN sich diese geeignet authentisieren. Die Authentisierung zwischen dem slapd-Server und den Kommunikationsbeteiligten MUSS verschlüsselt werden. Es SOLLTEN NUR die Hashwerte von Passwörtern auf den Clients und Servern abgespeichert werden. Es MUSS ein geeigneter Hashing-Algorithmus 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.2.3.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.3.A8 Einschränkungen von Attributen bei OpenLDAP (S)

Anhand von Overlays SOLLTEN die Attribute in OpenLDAP eingeschränkt werden. OpenLDAP SOLLTE so angepasst werden, dass Werte im Verzeichnisdienst nur einem bestimmten regulären Ausdruck entsprechen. Zudem SOLLTE mit Hilfe von Overlays sichergestellt werden, das ausgesuchte Werte nur einmal im Verzeichnisbaum vorhanden sind. Solche Restriktionen SOLLTEN ausschließlich auf Daten von Nutzenden angewendet werden.

APP.2.3.A9 Partitionierung und Replikation bei OpenLDAP (S)

Bei einer Partitionierung oder Replikation von OpenLDAP SOLLTE die Aufteilung geeignet für die Sicherheitsziele ausgewählt werden. Dabei SOLLTEN Veränderungen an den Daten durch Replikation zwischen den Servern ausgetauscht werden. Ein Replikationsmodus SOLLTE in Abhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen gewählt werden.

APP.2.3.A10 Sichere Aktualisierung von OpenLDAP (S)

Bei Updates SOLLTE darauf geachtet werden, ob die Änderungen eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten betreffen. Beim Update auf neue Releases SOLLTE geprüft werden, ob die verwendeten Overlays und Backends in der neuen Version weiterhin zur Verfügung stehen. Ist dies nicht der Fall, SOLLTEN geeignete Migrationspfade ausgewählt werden.

Setzen Administrierende eigene Skripte ein, SOLLTEN sie daraufhin überprüft werden, ob sie mit der aktualisierten Version von OpenLDAP problemlos zusammenarbeiten. Die Konfiguration und die Zugriffsrechte SOLLTEN nach einer Aktualisierung sorgfältig geprüft werden.

APP.2.3.A11 Einschränkung der OpenLDAP-Laufzeitumgebung (S)

Die Laufzeitumgebung des slapd-Servers SOLLTE, möglichst mit Mitteln des Betriebssystems, auf die minimal benötigten Dateien, Verzeichnisse und vom Betriebssystem bereitgestellten Funktionen eingeschränkt werden. Werden hierfür Containerisierungstechniken eingesetzt, SOLLTEN diese unter Berücksichtigung von SYS.1.6 *Containerisierung* genutzt werden. Wird der slapd-Server als exklusiver Dienst auf einem dedizierten Server betrieben, SOLLTE dieser ausreichend gehärtet sein.

APP.2.3.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.3.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.2.3 *OpenLDAP* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.1 Webanwendungen und Webservices

1. Beschreibung

1.1. Einleitung

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

Webservices sind Anwendungen, die das HTTP(S)-Protokoll verwenden, um Daten für andere Anwendungen bereitzustellen. In der Regel werden sie nicht unmittelbar durch Benutzende angesteuert.

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

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

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Webanwendungen und Webservices sicher einzusetzen sowie Informationen zu schützen, die durch sie verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf jede Webanwendung und jeden Webservice anzuwenden, die im Informationsverbund eingesetzt werden.

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.

Webservice-Schnittstellen werden oft via Representational State Transfer (REST) und Simple Object Access Protocol (SOAP) realisiert. In diesem Baustein werden nur REST-basierte Webservices betrachten. Der Fokus liegt dabei auf der Lebenszyklusphase „Betrieb". Sicherheitsanforderungen, die sich beispielsweise aus der Planung und Konzeption sowie Aussonderung und Notfallvorsorge ergeben, werden in diesem Baustein nicht betrachtet, sondern müssen gesondert im Rahmen einer Risikoanalyse ermittelt werden.

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

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.3.1 *Webanwendungen und Webservices* von besonderer Bedeutung.

2.1. Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung oder dem Webservice 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 und Webservices

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

2.3. Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn Funktionen einer Webanwendung oder eines Webservices automatisiert genutzt werden, können so zahlreiche Vorgänge in kurzer Zeit ausgeführt werden. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann so z. B. versucht werden, gültige Kombinationen von Konten und Passwörtern zu erraten (Brute-Force). Außerdem kann eine Liste mit gültigen Konten erzeugt werden (Enumeration), falls die Webanwendung oder der Webservice Informationen über vorhandene Konten 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 oder eines Webservices nur bestimmten Gruppen vorbehalten bleiben. Die entsprechenden Personen erhalten dann z. B. Konten, die exklusiv mit den notwendigen Zugriffsrechten ausgestattet sind. Unter diesen Konten authentisieren sich die Benutzenden zu Beginn jeder Sitzung in der Webanwendung oder dem Webservice, z. B. mit Kontoname und Passwort. Wird diese Authentisierung nicht korrekt konfiguriert, kann sie möglicherweise umgangen werden. Außerdem kann eine Webanwendung oder ein Webservice so konfiguriert werden, dass Zugangsdaten auf dem Webserver unsicher gespeichert werden. Im Falle eines erfolgreichen Angriffs verfügen Angreifende dann über große Mengen von Zugangsdaten, die sie auch an anderen Stellen einsetzen könnten.

3. Anforderungen

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

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.3.1.A1 Authentisierung (B)

Der IT-Betrieb MUSS Webanwendungen und Webservices so konfigurieren, dass sich Clients gegenüber der Webanwendung oder dem Webservice 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 (B)

Falls eine Webanwendung oder ein Webservice 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 Clients die Funktion verwenden dürfen. Auch MÜSSEN Zugriffs- und

Ausführungsrechte restriktiv gesetzt werden. Zudem MUSS sichergestellt werden, dass Clients Dateien nur im vorgegebenen erlaubten Speicherort speichern können.

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 (B)

Der IT-Betrieb MUSS sicherstellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei MUSS jedoch berücksichtigt werden, 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, 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 oder zum Webservice 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 oder des Webservices 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

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

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

APP.3.1.A9 Beschaffung von Webanwendungen und Webservices (S)

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

- 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 den Entwickelnden der Software,
- Schutzmechanismen vor verbreiteten Angriffen auf Webanwendungen und Webservices sowie
- Zugriff auf den Quelltext der Webanwendung oder des Webservices.

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 (S)

Webanwendungen und Webservices SOLLTEN 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 und Webservices 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 und Webservices 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 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.3.1.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 oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices 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 und Webservices 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.

Bundesamt
für Sicherheit in der
Informationstechnik

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 Webservers 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 Webservers 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 Webservers 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 Webservers 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.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.3 Fileserver

1. Beschreibung

1.1. Einleitung

Ein Fileserver (oder auch Dateiserver) ist ein Server in einem Netz, der Dateien von (internen) Festplatten oder Netzfestplatten für alle zugriffsberechtigten Personen sowie Clients zentral bereitstellt. Die Datenbestände können von den Zugriffsberechtigten genutzt werden, ohne sie z. B. auf Wechseldatenträgern zu transportieren oder per E-Mail zu verteilen. Dadurch, dass die Daten zentral vorgehalten werden, können sie strukturiert und in verschiedenen Verzeichnissen und Dateien bereitgestellt werden. Bei Fileservern können Zugriffsrechte auf die Dateien zentral vergeben werden. Auch die Datensicherung kann vereinfacht werden, wenn sich alle Informationen an einer zentralen Stelle befinden.

Ein Fileserver verwaltet meistens Massenspeicher, die mit ihm über Schnittstellen wie SCSI (Small Computer System Interface) oder SAS (Serial Attached SCSI) verbunden sind. Die Speicher befinden sich entweder direkt im Gehäuse des Fileservers oder sind extern angeschlossen. Letzteres wird oft als Directly Attached Storage (DAS) bezeichnet. Ein Fileserver kann auf herkömmlicher Server-Hardware oder einer dedizierten Appliance betrieben werden. Oft können bei großen Datenmengen auch zentrale Storage-Area-Network (SAN)-Speicher über Host-Bus-Adapter (HBA) im Server und an SAN-Switches angebunden werden.

1.2. Zielsetzung

In diesem Baustein werden wesentliche, für einen Fileserver spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Einsatz beschrieben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.3.*Fileserver* ist auf jeden Fileserver im Informationsverbund einmal anzuwenden.

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die beim Einsatz von Fileservern zu beachten und zu erfüllen sind. Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand des vorliegenden Bausteins, sondern werden im Baustein SYS1.1 *Allgemeiner Server* bzw. in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt, z. B. in SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server*. Es werden keine Anforderungen an netzbasierte Speichersysteme bzw. Speichernetze beschrieben. Diese sind im Baustein SYS.1.8 *Speicherlösungen* zu finden. Auch wird nicht auf dedizierte Dienste eingegangen, mit

denen ein Fileserver betrieben werden kann, wie z. B. Samba. Der Dienst Samba wird im Baustein APP.3.4 *Samba* behandelt.

Ein wichtiger Schwerpunkt bei der Absicherung eines Fileservers ist es, Zugriffsrechte auf Dateien nur restriktiv zu vergeben. Weitergehende Anforderungen hierzu sind in dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden. Auch die Sicherung der auf einem Fileserver abgelegten Informationen wird in diesem Baustein nicht behandelt. Hierzu sind die Anforderungen des Bausteins CON.3 *Datensicherungskonzept* zu erfüllen.

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.3.3 *Fileserver* von besonderer Bedeutung.

2.1. Ausfall eines Fileservers

Fällt ein Fileserver aus, kann der gesamte Informationsverbund davon betroffen sein und damit auch wichtige Geschäftsprozesse und Fachaufgaben der Institution. Nicht nur Benutzende, sondern auch Anwendungen können auf Daten vom Fileserver angewiesen sein, um ordnungsgemäß zu funktionieren. Ist die Verfügbarkeit von Daten und Diensten nicht gegeben, können z. B. Fristen nicht eingehalten oder essenzielle Geschäftsprozesse unterbrochen werden. Ist zudem kein Notfallmanagementkonzept vorhanden, können sich Wiederanlaufzeiten weiter erhöhen. In vielen Fällen führt dies zu finanziellen Einbußen. Außerdem kann sich der Ausfall auf andere Institutionen auswirken.

2.2. Unzureichende Dimensionierung des Fileservers

Ist die Leitungsanbindung oder die Speicherkapazität des Fileservers unzureichend, können sich die Zugriffszeiten erhöhen oder Speicherengpässe können auftreten. Dadurch können beispielsweise Mitarbeitende aufgrund der längeren Wartezeiten frustriert werden und damit beginnen, Daten lokal zu speichern. So kann nicht mehr nachvollzogen werden, wo Daten gespeichert sind und wer im Besitz der Daten ist. Auch Applikationen, die auf eine korrekte (Zwischen-)Speicherung von Informationen angewiesen sind, können nicht mehr zuverlässig funktionieren.

2.3. Unzureichende Überprüfung von abgelegten Dateien

Ist ein Fileserver unzureichend in das Konzept zum Schutz vor Schadprogrammen der Institution einbezogen, kann es passieren, dass unbemerkt Schadsoftware auf dem Fileserver abgelegt wird. Alle IT-Systeme und Anwendungen, die auf die Daten des Fileservers zugreifen, können mit der Schadsoftware infiziert werden, wodurch sich die Schadsoftware sehr schnell in der gesamten Institution ausbreitet.

2.4. Fehlendes oder unzureichendes Zugriffsberechtigungskonzept

Werden Zugriffsberechtigungen und Freigaben nicht ordnungsgemäß konzipiert und vergeben, können eventuell Dritte unbefugt auf Daten zugreifen. Dadurch können Unberechtigte Daten verändern, löschen oder kopieren.

2.5. Unstrukturierte Datenhaltung

Wird die Speicherstruktur nicht vorgegeben bzw. halten sich die Mitarbeitenden nicht daran, können Daten unübersichtlich und unkoordiniert auf dem Fileserver gespeichert werden. Das führt zu

verschiedenen Problemen, wie zum Beispiel Speicherplatzverschwendung durch das mehrmalige Ablegen derselben Datei. Auch können unterschiedliche Versionen einer Datei abgelegt werden. Außerdem sind unbefugte Zugriffe möglich, wenn sich z. B. Dateien in Verzeichnissen oder Dateisystemen befinden, die Dritten zugänglich gemacht werden.

2.6. Verlust von auf Fileservern abgespeicherten Daten

Fällt ein Fileserver komplett aus oder sind einzelne Komponenten defekt, können ohne eine Dateisynchronisierung oder ein funktionierendes Backup wichtige Informationen verloren gehen. Das gleiche gilt, wenn Mitarbeitende Dateien unbeabsichtigt löschen. Sollte zudem keine ausreichende Redundanz, etwa durch ein geeignetes Redundant Array of Independent Disks (RAID), eingesetzt werden, können weitere Probleme folgen. So wirkt sich der Ausfall eines einzelnen Datenträgers direkt auf den laufenden Betrieb aus, da die Dateien nicht mehr verfügbar sind.

2.7. Ransomware

Eine spezielle Form von Schadprogrammen ist Ransomware, bei der Daten auf den infizierten IT-Systemen verschlüsselt werden. Angreifende verlangen im Nachgang die Zahlung eines Lösegelds, damit das Opfer die Daten wieder entschlüsseln kann. Es ist jedoch auch nach der Zahlung eines Lösegelds nicht gewährleistet, dass die Daten wiederhergestellt werden können.

Nicht nur die lokalen Daten des infizierten IT-Systems werden hierbei verschlüsselt. Viele Ausprägungen von Ransomware suchen nach Netzlaufwerken mit Schreibzugriff, auf denen alle Daten ebenfalls verschlüsselt werden.

Damit können alle verschlüsselten Informationen seit der letzten Datensicherung verloren sein, auch wenn ein Lösegeld gezahlt wurde. Nicht nur das ursprünglich infizierte IT-System wäre hiervon betroffen, sondern auch zentral abgelegte Informationen, auf die viele IT-Systeme zugreifen dürfen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.3 *Fileserver* 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	Benutzende

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.3.3.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A2 Einsatz von RAID-Systemen (B)

Der IT-Betrieb MUSS festlegen, ob im Fileserver ein RAID-System eingesetzt werden soll. Eine Entscheidung gegen ein solches System MUSS nachvollziehbar dokumentiert werden. Falls ein RAID-System eingesetzt werden soll, MUSS der IT-Betrieb entscheiden:

- welches RAID-Level benutzt werden soll,
- wie lang die Zeitspanne für einen RAID-Rebuild-Prozess sein darf und
- ob ein Software- oder ein Hardware-RAID eingesetzt werden soll.

In einem RAID SOLLTEN Hotspare-Festplatten vorgehalten werden.

APP.3.3.A3 Einsatz von Viren-Schutzprogrammen (B)

Alle Daten MÜSSEN durch ein Viren-Schutzprogramm auf Schadsoftware untersucht werden, bevor sie auf dem Fileserver abgelegt werden.

APP.3.3.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A15 Planung von Fileservern (B)

Bevor eine Institution einen oder mehrere Fileserver einführt, SOLLTE sie entscheiden, wofür die Fileserver genutzt und welche Informationen darauf verarbeitet werden. Die Institution SOLLTE jede benutzte Funktion eines Fileservers einschließlich deren Sicherheitsaspekte planen. Arbeitsplatzrechner DÜRFEN NICHT als Fileserver eingesetzt werden.

Der Speicherplatz des Fileservers MUSS ausreichend dimensioniert sein. Auch ausreichende Speicherreserven SOLLTEN vorgehalten werden. Es SOLLTE ausschließlich Massenspeicher verwendet werden, der für einen Dauerbetrieb ausgelegt ist. Die Geschwindigkeit und die Anbindung der Massenspeicher MUSS für den Einsatzzweck angemessen sein.

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.3.3.A6 Beschaffung eines Fileservers und Auswahl eines Dienstes (S)

Die Fileserver-Software SOLLTE geeignet ausgewählt werden. Der Fileserver-Dienst SOLLTE den Einsatzzweck des Fileservers unterstützen, z. B. Einbindung von Netzlaufwerken in den Clients, Streaming von Multimedia-Inhalten, Übertragung von Boot-Images von festplattenlosen IT-Systemen oder ausschließliche Dateiübertragung über FTP. Die Leistung, die Speicherkapazität, die Bandbreite sowie die Anzahl der Benutzenden, die den Fileserver nutzen, SOLLTEN bei der Beschaffung des Fileservers berücksichtigt werden.

APP.3.3.A7 Auswahl eines Dateisystems (S)

Der IT-Betrieb SOLLTE eine Anforderungsliste erstellen, nach der die Dateisysteme des Fileservers bewertet werden. Das Dateisystem SOLLTE den Anforderungen der Institution entsprechen. Das Dateisystem SOLLTE eine Journaling-Funktion bieten. Auch SOLLTE es über einen Schutzmechanismus verfügen, der verhindert, dass mehrere Benutzende oder Anwendungen gleichzeitig schreibend auf eine Datei zugreifen.

APP.3.3.A8 Strukturierte Datenhaltung (S) [Benutzende]

Es SOLLTE eine Struktur festgelegt werden, nach der Daten abzulegen sind. Die Benutzenden SOLLTEN regelmäßig über die geforderte strukturierte Datenhaltung informiert werden. Die Dateien SOLLTEN ausschließlich strukturiert auf den Fileserver abgelegt werden. Es SOLLTE schriftlich festgelegt werden, welche Daten lokal und welche auf dem Fileserver gespeichert werden dürfen. Programm- und Arbeitsdaten SOLLTEN in getrennten Verzeichnissen gespeichert werden. Die Institution SOLLTE regelmäßig überprüfen, ob die Vorgaben zur strukturierten Datenhaltung eingehalten werden.

APP.3.3.A9 Sicheres Speichermanagement (S)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, ob die Massenspeicher des Fileservers noch wie vorgesehen funktionieren. Es SOLLTEN geeignete Ersatzspeicher vorgehalten werden.

Wurde eine Speicherhierarchie (Primär-, Sekundär- bzw. Tertiärspeicher) aufgebaut, SOLLTE ein (teil-)automatisiertes Speichermanagement verwendet werden. Werden Daten automatisiert verteilt, SOLLTE regelmäßig manuell überprüft werden, ob dies korrekt funktioniert.

Es SOLLTEN mindestens nicht-autorisierte Zugriffsversuche auf Dateien und Änderungen von Zugriffsrechten protokolliert werden.

APP.3.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.3.A11 Einsatz von Speicherbeschränkungen (S)

Der IT-Betrieb SOLLTE bei mehreren Benutzenden auf dem Fileserver prüfen, Beschränkungen des Speicherplatzes für einzelne Benutzende (Quotas) einzurichten. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystems genutzt werden, um die Benutzenden bei einem bestimmten Füllstand der Festplatte zu warnen oder in diesem Fall nur noch dem IT-Betrieb Schreibrechte einzuräumen.

APP.3.3.A14 Einsatz von Error-Correction-Codes (S)

Der IT-Betrieb SOLLTE ein fehlererkennendes bzw. fehlerkorrigierendes Dateisystem einsetzen. Hierfür SOLLTE genügend Speicherplatz vorgehalten werden. Der IT-Betrieb SOLLTE beachten, dass, je nach eingesetztem Verfahren, Fehler nur mit einer gewissen Wahrscheinlichkeit erkannt und auch nur in begrenzter Größenordnung behoben werden können.

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.3.3.A12 Verschlüsselung des Datenbestandes (H)

Die Massenspeicher des Fileservers SOLLTEN auf Dateisystem- oder Hardwareebene verschlüsselt werden. Falls Hardwareverschlüsselung eingesetzt wird, SOLLTEN Produkte verwendet werden, deren Verschlüsselungsfunktion zertifiziert wurde. Es SOLLTE sichergestellt werden, dass der Virenschutz die verschlüsselten Daten auf Schadsoftware prüfen kann.

APP.3.3.A13 Replikation zwischen Standorten (H)

Für hochverfügbare Fileserver SOLLTE eine angemessene Replikation der Daten auf mehreren Massenspeichern stattfinden. Daten SOLLTEN zudem zwischen unabhängigen Fileservern repliziert werden, die sich an unabhängigen Standorten befinden. Dafür SOLLTE vom IT-Betrieb ein geeigneter

Replikationsmechanismus ausgewählt werden. Damit die Replikation wie vorgesehen funktionieren kann, SOLLTEN hinreichend genaue Zeitdienste genutzt und betrieben werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.3.3 *Fileserver* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.4 Samba

1. Beschreibung

1.1. Einleitung

Samba ist ein frei verfügbarer und vollwertiger Active Directory Domain Controller (ADDC), der Authentisierungs-, Datei- und Druckdienste bereitstellen kann und dadurch die Interoperabilität zwischen der Windows- und der Unix-Welt ermöglicht. Samba führt viele unterschiedliche Protokolle und Techniken zusammen. Dazu gehört beispielsweise das Server-Message-Block (SMB)-Protokoll. Als Samba-Server werden Server bezeichnet, auf denen Samba betrieben wird. In der Regel sind das Unix-Server.

Wurde der Einsatz von Samba korrekt konzipiert und geeignet konfiguriert, interagiert Samba mit einem Windows-Client oder -Server, als ob es selbst ein Windows-System wäre.

1.2. Zielsetzung

Ziel des Bausteins ist es darzustellen, wie Samba in Institutionen sicher eingesetzt werden kann und wie sich die durch Samba bereitgestellten Informationen schützen lassen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.4.*Samba* ist auf jeden Samba-Server des betrachteten Informationsverbunds anzuwenden.

Dieser Baustein betrachtet Samba als Authentisierungs-, Datei- und Druckdienst. Da Samba in der Regel auf Unix-Servern eingesetzt wird und dort aus der Windows-Server-Welt bekannte Dienste bereitstellt, sind die Sicherheitsaspekte der Bausteine SYS.1.1 *Allgemeiner Server* und SYS.1.3 *Server unter Linux und Unix* zu berücksichtigen.

Ein wichtiger Schwerpunkt bei der Absicherung eines Samba-Servers ist es, Zugriffsrechte auf Dateien nur restriktiv zu vergeben. Vertiefende Informationen zum Identitäts- und Berechtigungsmanagement sind nicht in diesem Baustein, sondern in ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden.

Generelle Sicherheitsanforderungen für Drucker, Fileserver oder Verzeichnisdienste sind nicht Bestandteil dieses Bausteins. Diese werden in den Bausteinen SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte*, APP.3.3 *Fileserver* und APP.2.1 *Allgemeiner Verzeichnisdienst* sowie APP.2.3 *OpenLDAP* beschrieben.

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.3.4 *Samba* von besonderer Bedeutung.

2.1. Abhören ungeschützter Kommunikationsverbindungen von Samba

Wenn ungeschützte Kommunikationsverbindungen von Samba abgehört werden, können vertrauliche Informationen abgefangen und missbraucht werden. Beim Dateitransfer zwischen Unix-Servern, Windows-Servern und Clients werden oftmals Protokolle ohne umfangreiche Sicherheitseigenschaften eingesetzt, sodass sowohl Authentisierungs- als auch Nutzungsdaten für Dritte zugänglich sind und von Unberechtigten missbraucht werden könnten. Das kann dazu führen, dass schützenswerte Informationen der Institution in die falschen Hände gelangen.

2.2. Unsichere Standardeinstellungen auf Samba-Servern

Um einige Fähigkeiten des Samba-Servers zu zeigen und um den Administrierenden einen schnellen Einstieg zu ermöglichen, wird während der Installation des Samba-Servers die Konfigurationsdatei smb.conf mit Standardeinstellungen erzeugt. Mit den in dieser Datei voreingestellten Optionen kann der Samba-Server im Anschluss gestartet werden. Wird diese Datei unbedacht ohne weitere Anpassungen benutzt, kann das zu erheblichen Sicherheitslücken führen. Werden die beispielhaft vorgenommenen Dateifreigaben nicht auskommentiert, können in diesen unerwünschten Freigaben sensible Informationen eingesehen werden.

2.3. Unberechtigte Nutzung oder Administration von Samba

Unbefugte können durch die Nutzung von Anwendungen oder IT-Systemen an vertrauliche Informationen gelangen, diese manipulieren oder Störungen verursachen. So ist es möglich, dass sie Samba unberechtigt administrieren können. Besonders kritisch ist es, wenn veraltete und nicht mehr aktualisierte Konfigurationswerkzeuge eingesetzt werden, wie z. B. das Samba Web Administration Tool (SWAT).

2.4. Fehlerhafte Administration von Samba

Sind die Administrierenden mit den umfangreichen Komponenten, Funktionen, Optionen und Konfigurationseinstellungen von Samba zu wenig vertraut, kann dies zu weitreichenden Komplikationen führen. So können Fehlkonfigurationen des DNS oder des Berechtigungsmanagements dazu führen, dass Unbefugte auf Ressourcen zugreifen können. Des Weiteren kann dies zu Betriebsunterbrechungen führen oder es können schützenswerte Informationen offengelegt werden.

2.5. Datenverlust bei Samba

Ein Datenverlust wirkt sich erheblich auf den IT-Einsatz aus. Wenn institutionsrelevante Informationen zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder gar nicht mehr ausgeführt werden. Bei Samba ist beispielsweise zu beachten, dass sich die Eigenschaften der Dateisysteme unter Windows und Unix erheblich voneinander unterscheiden. Deswegen ist nicht immer sichergestellt, dass die Zugriffsrechte unter Windows aufrechterhalten bleiben, unter Umständen können so wichtige Dateieigenschaften verloren gehen. Auch können

dadurch Informationen zu sogenannten Alternate Data Streams (ADS) und DOS-Attributen verloren gehen.

2.6. Integritätsverlust schützenswerter Informationen bei Samba

Samba selbst legt wichtige Betriebsdaten in Datenbanken im Trivial-Database-(TDB)-Format ab. Sollten diese Datenbanken vom Betriebssystem nicht ausreichend leistungsfähig und konsistent behandelt werden, können sie Probleme verursachen, wenn Samba-Dienste genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.4 *Samba* 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	Keine

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.3.4.A1 Planung des Einsatzes eines Samba-Servers (B)

Der IT-Betrieb MUSS die Einführung eines Samba-Servers sorgfältig planen und regeln. Der IT-Betrieb MUSS abhängig vom Einsatzszenario definieren, welche Aufgaben der Samba-Server zukünftig erfüllen soll und in welcher Betriebsart er betrieben wird. Außerdem MUSS festgelegt werden, welche Komponenten von Samba und welche weiteren Komponenten dafür erforderlich sind.

Soll die Cluster-Lösung CTDB (Cluster Trivia Data Base) eingesetzt werden, MUSS der IT-Betrieb diese Lösung sorgfältig konzeptionieren. Falls Samba die Active-Directory-(AD)-Dienste auch für Linux- und Unix-Systeme bereitstellen soll, MÜSSEN diese Dienste ebenfalls sorgfältig geplant und getestet werden. Des Weiteren MUSS das Authentisierungsverfahren für das AD sorgfältig konzipiert und implementiert werden. Die Einführung und die Reihenfolge, in der die Stackable-Virtual-File-System-(VFS)-Module ausgeführt werden, MUSS sorgfältig konzipiert werden. Die Umsetzung SOLLTE dokumentiert werden.

Soll IPv6 unter Samba eingesetzt werden, MUSS auch dies sorgfältig geplant werden. Zudem MUSS in einer betriebsnahen Testumgebung überprüft werden, ob die Integration fehlerfrei funktioniert.

APP.3.4.A2 Sichere Grundkonfiguration eines Samba-Servers (B)

Der IT-Betrieb MUSS den Samba-Server sicher konfigurieren. Hierfür MÜSSEN unter anderem die Einstellungen für die Zugriffskontrollen angepasst werden. Das gleiche SOLLTE auch für Einstellungen gelten, welche die Leistungsfähigkeit des Servers beeinflussen.

Samba MUSS vom IT-Betrieb so konfiguriert werden, dass Verbindungen nur von sicheren Hosts und Netzen entgegengenommen werden. Änderungen an der Konfiguration SOLLTEN sorgfältig dokumentiert werden, sodass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat. Dabei MUSS nach jeder Änderung überprüft werden, ob die Syntax der Konfigurationsdatei noch korrekt ist.

Zusätzliche Softwaremodule wie SWAT DÜRFEN NICHT installiert 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.3.4.A3 Sichere Konfiguration eines Samba-Servers (S)

Datenbanken im Trivial-Database-(TDB)-Format SOLLTEN NICHT auf einer Partition gespeichert werden, die ReiserFS als Dateisystem benutzt. Wird eine netlogon-Freigabe konfiguriert, SOLLTEN unberechtigte Benutzende KEINE Dateien in dieser Freigabe modifizieren können.

Das Betriebssystem eines Samba-Servers SOLLTE Access Control Lists (ACLs) in Verbindung mit dem eingesetzten Dateisystem unterstützen. Zusätzlich SOLLTE sichergestellt werden, dass das Dateisystem mit den passenden Parametern eingebunden wird.

Die Voreinstellungen von SMB Message Signing SOLLTEN beibehalten werden, sofern sie nicht im Widerspruch zu den existierenden Sicherheitsrichtlinien im Informationsverbund stehen.

APP.3.4.A4 Vermeidung der NTFS-Eigenschaften auf einem Samba-Server (S)

Wird eine Version von Samba eingesetzt, die im New Technology File System (NTFS) keine ADS abbilden kann und sollen Dateisystemobjekte über Systemgrenzen hinweg kopiert oder verschoben werden, SOLLTEN Dateisystemobjekte KEINE ADS mit wichtigen Informationen enthalten.

APP.3.4.A5 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server (S)

Die von Samba standardmäßig verwendeten Parameter, mit denen DOS-Attribute auf das Unix-Dateisystem abgebildet werden, SOLLTEN NICHT verwendet werden. Stattdessen SOLLTE Samba so konfiguriert werden, dass es DOS-Attribute und die Statusindikatoren zur Vererbung (Flag) in Extended Attributes speichert. Die Freigaben SOLLTEN ausschließlich über die Samba-Registry verwaltet werden.

Ferner SOLLTEN die effektiven Zugriffsberechtigungen auf die Freigaben des Samba-Servers regelmäßig überprüft werden.

APP.3.4.A6 Sichere Konfiguration von Winbind unter Samba (S)

Für jedes Domänen-Konto einer Windows-Domäne SOLLTE im Betriebssystem des Servers ein Konto mit allen notwendigen Gruppenmitgliedschaften vorhanden sein. Falls das nicht möglich ist, SOLLTE Winbind eingesetzt werden, um Domänen-Konten in Unix-Konten umsetzen. Beim Einsatz von Winbind SOLLTE sichergestellt werden, dass Kollisionen zwischen lokalen Benutzenden in Unix und Benutzenden in der Domäne verhindert werden.

Des Weiteren SOLLTEN die PAM (Pluggable Authentication Modules) eingebunden werden.

APP.3.4.A7 Sichere Konfiguration von DNS unter Samba (S)

Wenn Samba als DNS-Server eingesetzt wird, SOLLTE die Einführung sorgfältig geplant und die Umsetzung vorab getestet werden. Da Samba verschiedene AD-Integrationsmodi unterstützt, SOLLTE der IT-Betrieb die DNS-Einstellungen entsprechend dem Verwendungsszenario von Samba vornehmen.

APP.3.4.A8 Sichere Konfiguration von LDAP unter Samba (S)

Werden die Benutzenden unter Samba mit LDAP verwaltet, SOLLTE die Konfiguration sorgfältig vom IT-Betrieb geplant und dokumentiert werden. Die Zugriffsberechtigungen auf das LDAP SOLLTEN mittels ACLs geregelt werden.

APP.3.4.A9 Sichere Konfiguration von Kerberos unter Samba (S)

Zur Authentisierung SOLLTE das von Samba implementierte Heimdal Kerberos Key Distribution Center (KDC) verwendet werden. Es SOLLTE darauf geachtet werden, dass die von Samba vorgegebene Kerberos-Konfigurationsdatei verwendet wird. Es SOLLTEN nur sichere Verschlüsselungsverfahren für Kerberos-Tickets benutzt werden.

Wird mit Kerberos authentisiert, SOLLTE der zentrale Zeitserver lokal auf dem Samba-Server installiert werden. Der NTP-Dienst SOLLTE so konfiguriert werden, dass nur autorisierte Clients die Zeit abfragen können.

APP.3.4.A10 Sicherer Einsatz externer Programme auf einem Samba-Server (S)

Vom IT-Betrieb SOLLTE sichergestellt werden, dass Samba nur auf schadhafte Funktionen überprüfte und vertrauenswürdige externe Programme aufruft.

APP.3.4.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.4.A12 Schulung der Administrierenden eines Samba-Servers (S)

Die Administrierenden SOLLTEN zu den genutzten spezifischen Bereichen von Samba wie z. B. Benutzendenauthentisierung, Windows- und Unix-Rechtemodelle, aber auch zu NTFS ACLs und NTFS ADS geschult werden.

APP.3.4.A13 Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers (S)

Es SOLLTEN alle Systemkomponenten in das institutionsweite Datensicherungskonzept eingebunden werden, die erforderlich sind, um einen Samba-Server wiederherzustellen. Auch die Kontoinformationen aus allen eingesetzten Backends SOLLTEN berücksichtigt werden. Ebenso SOLLTEN alle TDB-Dateien gesichert werden. Des Weiteren SOLLTE die Samba-Registry mit gesichert werden, falls sie für Freigaben eingesetzt wurde.

APP.3.4.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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.3.4.A15 Verschlüsselung der Datenpakete unter Samba (H)

Um die Sicherheit der Datenpakete auf dem Transportweg zu gewährleisten, SOLLTEN die Datenpakete mit den ab SMB Version 3 integrierten Verschlüsselungsverfahren verschlüsselt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.3.4 *Samba* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.6 DNS-Server

1. Beschreibung

1.1. Einleitung

Domain Name System (DNS) ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. DNS kann mit einem Telefonbuch verglichen werden, das Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Üblicherweise wird über DNS zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet.

Welche Hostnamen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für das IT-System benutzt, auf dem diese Software betrieben wird.

DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch häufig im internen Netz einer Institution eingesetzt. Auf den IT-Systemen der Benutzenden sind standardmäßig sogenannte Resolver installiert. Über den Resolver werden die Anfragen an DNS-Server gestellt. Als Antwort liefern die DNS-Server Informationen über den Domain-Namensraum zurück.

DNS-Server können nach ihren Aufgaben unterschieden werden. Dabei gibt es grundsätzlich zwei verschiedenen Typen: Advertising DNS-Server und Resolving DNS-Server. Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz einer Institution.

Der Ausfall eines DNS-Servers kann sich gravierend auf den Betrieb einer IT-Infrastruktur auswirken. Dabei ist nicht das ausgefallene DNS-System an sich problematisch, sondern die DNS-basierten Dienste, die daraus eingeschränkt werden. Unter Umständen sind Webserver oder E-Mail-Server nicht mehr erreichbar oder die Fernwartung funktioniert nicht mehr. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede Zone betrieben werden.

1.2. Zielsetzung

In diesem Baustein werden die für einen DNS-Server spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Einsatz beschrieben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.6 *DNS-Server* ist auf jeden im Informationsverbund eingesetzten DNS-Server anzuwenden.

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn eine Institution DNS-Server einsetzt. Der Fokus liegt dabei auf der Verfügbarkeit von DNS-Servern und der Integrität der übertragenen Informationen. Außerdem werden Probleme behandelt, die auftreten können, wenn DNS-Server eingesetzt werden.

Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand dieses Bausteins. Diese werden im Baustein SYS1.1 *Allgemeiner Server* und in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt, z. B. SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server*.

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.3.6 *DNS-Server* von besonderer Bedeutung.

2.1. Ausfall des DNS-Servers

Fällt ein DNS-Server aus, kann der gesamte IT-Betrieb davon betroffen sein. Da Clients und andere Server der Institution dann nicht mehr in der Lage sind, interne und externe Adressen auf Basis der Hostnamen aufzulösen, können keine Datenverbindungen mehr aufgebaut werden. Auch externe IT-Systeme, z. B. von mobilen Mitarbeitenden, der Kundschaft sowie Geschäftspartnern und Geschäftspartnerinnen, können nicht auf die Server der Institution zugreifen. Dadurch sind in der Regel essenzielle Geschäftsprozesse gestört.

2.2. Unzureichende Leitungskapazitäten

Reichen die Leitungskapazitäten für einen DNS-Server nicht aus, können sich die Zugriffszeiten auf interne und externe Dienste erhöhen. Dadurch sind diese eventuell nur eingeschränkt oder gar nicht mehr nutzbar. Auch kann der DNS-Server dann leichter durch einen Denial-of-Service-(DoS)-Angriff überlastet werden.

2.3. Fehlende oder unzureichende Planung des DNS-Einsatzes

Fehler in der Planung stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der DNS-Einsatz nicht oder nur unzureichend geplant, kann dies zu Problemen und Sicherheitslücken im laufenden Betrieb führen. Sind beispielsweise die Firewall-Regeln, die den DNS-Verkehr steuern, zu freizügig definiert, kann dies unter Umständen einen Angriff zur Folge haben. Sind die Regeln jedoch zu restriktiv formuliert, können legitime Clients keine Anfragen an die DNS-Server stellen und werden beeinträchtigt, wenn sie etwa Dienste wie E-Mail oder FTP benutzen.

2.4. Fehlerhafte Domain-Informationen

Selbst wenn der DNS-Einsatz sorgfältig geplant und somit alle sicherheitsrelevanten Punkte berücksichtigt wurden, ist das nicht ausreichend, wenn semantisch sowie syntaktisch fehlerhafte Domain-Informationen erstellt werden. Dies gilt beispielsweise dann, wenn einem Hostnamen eine falsche IP-Adresse zugeordnet wird, Daten fehlen, nicht erlaubte Zeichen verwendet werden oder die

Vorwärts- und Rückwärtsauflösung inkonsistent sind. Enthalten Domain-Informationen Fehler, funktionieren Dienste, die diese Informationen benutzen, aufgrund der Falschinformationen nur eingeschränkt.

2.5. Fehlerhafte Konfiguration eines DNS-Servers

Sicherheitskritische Standardeinstellungen, selbst konfigurierte sicherheitskritische Einstellungen oder fehlerhafte Konfigurationen können dazu führen, dass ein DNS-Server nicht ordnungsgemäß funktioniert. Ist beispielsweise ein Resolving DNS-Server so konfiguriert, dass er rekursive Anfragen uneingeschränkt entgegennimmt, also sowohl aus dem internen Datennetz als auch aus dem Internet, kann aufgrund der erhöhten Last die Verfügbarkeit des Servers stark beeinträchtigt sein. Zusätzlich könnte er dadurch anfällig für DNS-Reflection-Angriffe werden.

Ebenso besteht bei fehlerhaft konfigurierten DNS-Servern die Gefahr, dass die Zonentransfers nicht auf berechtigte DNS-Server beschränkt sind. Damit kann jeder Host, der die Möglichkeit hat, eine Anfrage an die DNS-Server zu stellen, die gesamten Domain-Informationen dieser Server auslesen. Die so gewonnenen Daten können spätere Angriffe erleichtern.

2.6. DNS-Manipulation

Mit einem DNS-Cache-Poisoning-Angriff wird das Ziel verfolgt, dass das angegriffene IT-System falsche Zuordnungen von IP-Adressen und Namen speichert. Dabei wird ausgenutzt, dass DNS-Server erhaltene Domain-Informationen für einen gewissen Zeitraum im Cache zwischenspeichern. So können sich gefälschte Daten weiträumig verbreiten. Werden dann entsprechende Anfragen an den manipulierten DNS-Server gestellt, liefert dieser als Antwort die gefälschten Daten. Das IT-System, das diese Antwort empfängt, speichert diese zwischen und sein Cache ist somit ebenfalls „vergiftet“. Die gespeicherten Daten haben eine definierte Haltbarkeit (Time-To-Live, TTL). Wird der Resolving DNS-Server nach einer manipulierten Adresse gefragt, so wird er erst dann wieder einen anderen DNS-Server anfragen, wenn die Haltbarkeit abgelaufen ist. So können sich manipulierte DNS-Informationen lange halten, obwohl sie auf dem ursprünglich angegriffenen DNS-Server bereits wieder korrigiert sind. Gelingt es Angreifenden beispielsweise, die Namensauflösung für eine Domain zu übernehmen, indem sie die Einträge so manipulieren, dass ihre DNS-Server befragt werden, sind alle Subdomains automatisch mitbetroffen. DNS-Cache-Poisoning-Angriffe werden oft mit dem Ziel geführt, Anfragen auf bösartige Server umzuleiten.

2.7. DNS-Hijacking

DNS-Hijacking ist eine Angriffsmethode, die verwendet wird, um die Kommunikation zwischen Advertising DNS-Servern und Resolvern über das IT-System der Angreifenden zu leiten. Den Angreifenden ist es mit dieser Man-in-the-Middle-Attacke möglich, die Kommunikation zwischen den Servern abzuhören und aufzuzeichnen. Die weitaus größere Gefahr besteht jedoch darin, dass bei einem erfolgreichen Angriff jeglicher Datenverkehr zwischen den beiden IT-Systemen beliebig verändert werden kann. Wird nach einem erfolgreichen DNS-Hijacking-Angriff vom Resolver eines Clients eine Anfrage an einen DNS-Server gesendet, können Angreifende beispielsweise die Zuordnung von Namen und IP-Adresse ändern. DNS-Hijacking lässt sich auch mit anderen Angriffen kombinieren, zum Beispiel mit Phishing.

2.8. DNS-DoS

Bei einem DoS-Angriff auf einen DNS-Server werden so viele Anfragen an ihn gesendet, dass die Netzverbindung zum DNS-Server bzw. der DNS-Server selbst überlastet wird. In der Regel werden die Anfragen über Botnetze versendet, um die notwendige Datenrate zu erreichen. Ein auf diese Weise überlasteter DNS-Server kann keine legitimen Anfragen mehr beantworten.

2.9. DNS-Reflection

Bei einem DNS-Reflection-Angriff handelt es sich um einen DoS-Angriff, bei dem nicht der DNS-Server, an den die Anfragen gestellt werden, das Ziel ist, sondern das IT-System, das die Antworten empfängt. Dabei wird ausgenutzt, dass bestimmte Anfragen eine verhältnismäßig große Antwortdatenmenge erzeugen. Es ist dabei möglich, einen Verstärkungsfaktor von 100 und mehr zu erreichen. Das bedeutet, dass die Antwort, gemessen in Bytes, mindestens einhundert Mal größer ist als die Anfrage. Durch die Anzahl und Größe der Antworten wird die Netzbandbreite bzw. das empfangende IT-System selbst über seine Leistungskapazität hinaus überlastet. Somit kann jede beliebige technische IT-Komponente das Angriffsziel sein. DNS-Reflection-Angriffe werden durch Open Resolver begünstigt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.6 *DNS-Server* 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	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.3.6.A1 Planung des DNS-Einsatzes (B)

Der Einsatz von DNS-Servern MUSS sorgfältig geplant werden. Es MUSS zuerst festgelegt werden, wie der Netzdienst DNS aufgebaut werden soll. Es MUSS festgelegt werden, welche Domain-Informationen schützenswert sind. Es MUSS geplant werden, wie DNS-Server in das Netz des Informationsverbunds eingebunden werden sollen. Die getroffenen Entscheidungen MÜSSEN geeignet dokumentiert werden.

APP.3.6.A2 Einsatz redundanter DNS-Server (B)

Advertising DNS-Server MÜSSEN redundant ausgelegt werden. Für jeden Advertising DNS-Server MUSS es mindestens einen zusätzlichen Secondary DNS-Server geben.

APP.3.6.A3 Verwendung von separaten DNS-Servern für interne und externe Anfragen (B)

Advertising DNS-Server und Resolving DNS-Server MÜSSEN serverseitig getrennt sein. Die Resolver der internen IT-Systeme DÜRFEN NUR die internen Resolving DNS-Server verwenden.

APP.3.6.A4 Sichere Grundkonfiguration eines DNS-Servers (B)

Ein Resolving DNS-Server MUSS so konfiguriert werden, dass er ausschließlich Anfragen aus dem internen Netz akzeptiert. Wenn ein Resolving DNS-Server Anfragen versendet, MUSS er zufällige

Source Ports benutzen. Sind DNS-Server bekannt, die falsche Domain-Informationen liefern, MUSS der Resolving DNS-Server daran gehindert werden, Anfragen dorthin zu senden. Ein Advertising DNS-Server MUSS so konfiguriert werden, dass er Anfragen aus dem Internet immer iterativ behandelt.

Es MUSS sichergestellt werden, dass DNS-Zonentransfers zwischen Primary und Secondary DNS-Servern funktionieren. Zonentransfers MÜSSEN so konfiguriert werden, dass diese nur zwischen Primary und Secondary DNS-Servern möglich sind. Zonentransfers MÜSSEN auf bestimmte IP-Adressen beschränkt werden. Die Version des verwendeten DNS-Server-Produktes MUSS verborgen werden.

APP.3.6.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.6.A6 Absicherung von dynamischen DNS-Updates (B)

Es MUSS sichergestellt werden, dass nur legitimierte IT-Systeme Domain-Informationen ändern dürfen. Es MUSS festgelegt werden, welche Domain-Informationen die IT-Systeme ändern dürfen.

APP.3.6.A7 Überwachung von DNS-Servern (B)

DNS-Server MÜSSEN laufend überwacht werden. Es MUSS überwacht werden, wie ausgelastet die DNS-Server sind, um rechtzeitig die Leistungskapazität der Hardware anpassen zu können. DNS-Server MÜSSEN so konfiguriert werden, dass mindestens die folgenden sicherheitsrelevanten Ereignisse protokolliert werden:

- Anzahl der DNS-Anfragen,
- Anzahl der Fehler bei DNS-Anfragen,
- EDNS-Fehler (EDNS - Extension Mechanisms for DNS),
- auslaufende Zonen sowie
- fehlgeschlagene Zonentransfers.

APP.3.6.A8 Verwaltung von Domainnamen (B) [Zentrale Verwaltung]

Es MUSS sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Institution benutzt werden, regelmäßig und rechtzeitig verlängert werden. Eine Person MUSS bestimmt werden, die dafür zuständig ist, die Internet-Domainnamen zu verwalten. Falls Dienstleistende mit der Domainverwaltung beauftragt werden, MUSS darauf geachtet werden, dass die Institution die Kontrolle über die Domains behält.

APP.3.6.A9 Erstellen eines Notfallplans für DNS-Server (B)

Ein Notfallplan für DNS-Server MUSS erstellt werden. Der Notfallplan für DNS-Server MUSS in die bereits vorhandenen Notfallpläne der Institution integriert werden. Im Notfallplan für DNS-Server MUSS ein Datensicherungskonzept für die Zonen- und Konfigurationsdateien beschrieben sein. Das Datensicherungskonzept für die Zonen- und Konfigurationsdateien MUSS in das existierende Datensicherungskonzept der Institution integriert werden. Der Notfallplan für DNS-Server MUSS einen Wiederanlaufplan für alle DNS-Server im Informationsverbund enthalten.

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.3.6.A10 Auswahl eines geeigneten DNS-Server-Produktes (S)

Wird ein DNS-Server-Produkt beschafft, dann SOLLTE darauf geachtet werden, dass es sich in der Praxis ausreichend bewährt hat. Das DNS-Server-Produkt SOLLTE die aktuellen RFC-Standards

unterstützen. Das DNS-Server-Produkt SOLLTE die Zuständigen dabei unterstützen, syntaktisch korrekte Master Files zu erstellen.

APP.3.6.A11 Ausreichende Dimensionierung der DNS-Server (S)

Die Hardware des DNS-Servers SOLLTE ausreichend dimensioniert sein. Die Hardware des DNS-Servers SOLLTE ausschließlich für den Betrieb dieses DNS-Servers benutzt werden. Die Netzanbindungen sämtlicher DNS-Server im Informationsverbund SOLLTEN ausreichend bemessen sein.

APP.3.6.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.6.A13 Einschränkung der Sichtbarkeit von Domain-Informationen (S)

Der Namensraum eines Informationsverbunds SOLLTE in einen öffentlichen und einen institutionsinternen Bereich aufgeteilt werden. Im öffentlichen Teil SOLLTEN nur solche Domain-Informationen enthalten sein, die von Diensten benötigt werden, die von extern erreichbar sein sollen. IT-Systeme im internen Netz SOLLTEN selbst dann keinen von außen auflösbaren DNS-Namen erhalten, wenn sie eine öffentliche IP-Adresse besitzen.

APP.3.6.A14 Platzierung der Nameserver (S)

Primary und Secondary Advertising DNS-Server SOLLTEN in verschiedenen Netzsegmenten platziert werden.

APP.3.6.A15 Auswertung der Logdaten (S)

Die Logdateien des DNS-Servers SOLLTEN regelmäßig überprüft werden. Die Logdateien des DNS-Servers SOLLTEN regelmäßig ausgewertet werden. Mindestens die folgenden sicherheitsrelevanten Ereignisse SOLLTEN ausgewertet werden:

- Anzahl der DNS-Anfragen,
- Anzahl der Fehler bei DNS-Anfragen,
- EDNS-Fehler,
- auslaufende Zonen,
- fehlgeschlagene Zonentransfers sowie
- Veränderungen im Verhältnis von Fehlern zu DNS-Anfragen.

APP.3.6.A16 Integration eines DNS-Servers in eine "P-A-P"-Struktur (S)

Die DNS-Server SOLLTEN in eine „Paketfilter - Application-Level-Gateway - Paketfilter“-(P-A-P)-Struktur integriert werden (siehe auch NET.1.1 *Netzarchitektur und -design*). Der Advertising DNS-Server SOLLTE in diesem Fall in einer demilitarisierten Zone (DMZ) des äußeren Paketfilters angesiedelt sein. Der Resolving DNS-Server SOLLTE in einer DMZ des inneren Paketfilters aufgestellt sein.

APP.3.6.A17 Einsatz von DNSSEC (S)

Die DNS-Protokollerweiterung DNSSEC SOLLTE sowohl auf Resolving DNS-Servern als auch auf Advertising DNS-Servern aktiviert werden. Die dabei verwendeten Schlüssel Key-Signing-Keys (KSK) und Zone-Signing-Keys (ZSK) SOLLTEN regelmäßig gewechselt werden.

APP.3.6.A18 Erweiterte Absicherung von Zonentransfers (S)

Um Zonentransfers stärker abzusichern, SOLLTEN zusätzlich Transaction Signatures (TSIG) eingesetzt werden.

APP.3.6.A19 Aussonderung von DNS-Servern (S)

Der DNS-Server SOLLTE sowohl aus dem Domain-Namensraum als auch aus dem Netzverbund gelöscht werden.

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.3.6.A20 Prüfung des Notfallplans auf Durchführbarkeit (H)

Es SOLLTE regelmäßig überprüft werden, ob der Notfallplan für DNS-Server durchführbar ist.

APP.3.6.A21 Hidden Master (H)

Um Angriffe auf den primären Advertising DNS-Server zu erschweren, SOLLTE eine sogenannte Hidden-Master-Anordnung vorgenommen werden.

APP.3.6.A22 Anbindung der DNS-Server über unterschiedliche Provider (H)

Extern erreichbare DNS-Server SOLLTEN über unterschiedliche Provider angebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld DNS veröffentlicht:

- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 055: „Sichere Bereitstellung von DNS-Diensten: Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen“
- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 121: „Umsetzung von DNSSEC: Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions“
- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-81-2 „Secure Domain Name System (DNS) - Deployment Guide“ Empfehlungen zum Einsatz von DNS.

Im Request for Comments (RFC) bietet der RFC 1034 „Domain Names - Concepts and Facilities“ weiterführende Informationen zu DNS.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.4.2 SAP-ERP-System

1. Beschreibung

1.1. Einleitung

Enterprise-Resource-Planning-Systeme von SAP (kurz SAP-ERP-Systeme) werden eingesetzt, um interne und externe Geschäftsabläufe zu automatisieren und technisch zu unterstützen. SAP-ERP-Systeme verarbeiten daher typischerweise vertrauliche Informationen, sodass alle Komponenten und Daten geeignet geschützt werden müssen.

SAP-ERP-Systeme sind aktuell unter den Produktbezeichnungen SAP Business Suite und SAP S/4HANA auf dem Markt. Ein SAP-ERP-System setzt sich aus verschiedenen Modulen zusammen, mit denen die Organisationsstruktur einer Institution abgebildet werden kann. Zu den Modulen eines SAP-ERP-Systems zählen unter anderem Rechnungswesen, Personalwirtschaft und Logistik. Die Kernkomponenten des SAP-ERP-Systems sind SAP NetWeaver (Applikationsserver-Middleware) und SAP HANA (Applikationsserver und Datenbank). SAP NetWeaver ermöglicht es, SAP-ABAP- und SAP-JAVA-Anwendungen anzubinden und Prozesse systemweit zu steuern. SAP HANA kann in Echtzeit große Datenmengen für alle Geschäftsbereiche analysieren.

1.2. Zielsetzung

Der Baustein beschreibt, welche Gefährdungen für SAP-ERP-Systeme zu beachten sind und wie diese Systeme sicher installiert, konfiguriert und betrieben werden können. Er richtet sich an Informationssicherheitsbeauftragte und Administrierende, die dafür zuständig sind, SAP-ERP-Systeme zu planen und umzusetzen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.4.2 *SAP-ERP-System* ist auf jedes SAP-ERP-System anzuwenden.

Der Baustein beschränkt sich auf die Kerninstallation eines SAP-ERP-Systems und fokussiert die spezifischen Merkmale des darunterliegenden SAP-NetWeaver-Applikationsservers. Auch werden in diesem Baustein nicht alle verfügbaren SAP-Produkte detailliert beschrieben. Die folgenden Darstellungen beschränken sich auf die Konfiguration der SAP-Basis und gehen nicht auf Module oder Applikationen ein.

Anforderungen an die Entwicklung von ABAP-Programmen finden sich im Baustein APP.4.6 *SAP ABAP-Programmierung*. Darüber hinaus werden keine angrenzenden IT-Systeme, Betriebssysteme oder Datenbanken näher betrachtet. Dazu sind die spezifischen Bausteine wie SYS1.2.2 *Windows Server*

2012, SYS.1.3 *Server unter Linux und Unix* oder APP.4.3 *Relationale Datenbanken* anzuwenden. Ebenso geht der vorliegende Baustein nicht auf SAP HANA ein. Auf aktuelle Bezeichnungen der Produkte wird bewusst verzichtet, da sich diese häufig ändern.

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.4.2 *SAP-ERP-System* von besonderer Bedeutung:

2.1. Fehlende Berücksichtigung der Sicherheitsempfehlungen von SAP

Wird ein SAP-ERP-System aufgebaut, ohne dabei die empfohlenen Sicherheitsleitfäden von SAP zu berücksichtigen, kann das zu schweren Sicherheitsproblemen im System führen. Das ist z. B. der Fall, wenn SAP-Empfehlungen für das Konten- und Berechtigungsmanagement nicht korrekt umgesetzt werden. Auch wenn solche SAP-Empfehlungen ignoriert werden, welche die Kommunikation oder den Schnittstellenbetrieb mittels RFC und Webservices schützen, können Schwachstellen auftreten. Dadurch kann das gesamte System angreifbar sein.

2.2. Fehlendes oder nicht zeitnahes Einspielen von Patches und SAP-Sicherheitshinweisen

SAP-ERP-Systeme bestehen aus unterschiedlichen Modulen und Komponenten und sind komplexe Systeme, die meist sensible Daten verarbeiten. SAP veröffentlicht daher regelmäßig Patches und Sicherheitshinweise, um Softwarefehler und bekannt gewordene Schwachstellen zu beheben. Wenn neue Patches oder SAP-Sicherheitshinweise nicht zeitnah oder gar nicht eingespielt werden, könnten offene Sicherheitslücken von Angreifenden ausgenutzt werden. Dadurch könnten Angreifende SAP-ERP-Systeme manipulieren. Dann könnten vertrauliche Daten abfließen, Dienste ausfallen oder ganze Geschäftsprozesse stillstehen.

2.3. Mangelnde Planung, Umsetzung und Dokumentation eines SAP-Berechtigungskonzeptes

SAP-Berechtigungskonzepte sind fachlich und technisch komplex. Aufgrund dieser hohen Anforderungen werden sie in vielen Institutionen kaum oder nur ungenügend geplant und umgesetzt. Fehlt jedoch ein durchdachtes Berechtigungskonzept, werden z. B. Konten oft mehr Berechtigungen als notwendig zugewiesen. Diese Konten könnten dann das SAP-ERP-System vorsätzlich manipulieren oder versehentlich beschädigen. Somit ist die Integrität, Vertraulichkeit und Verfügbarkeit gefährdet.

Darüber hinaus muss das Design der Berechtigungen in S/4HANA-Systemen zwischen den integrierten Komponenten ABAP, HANA und NetWeaver Gateway (für Fiori-Anwendungen) genau abgestimmt und synchronisiert werden, da ansonsten widersprüchliche Berechtigungen vergeben werden könnten.

Wird das SAP-Berechtigungskonzept nicht ausreichend dokumentiert, können vergebene Berechtigungen nicht mehr nachvollzogen und somit gepflegt werden. So ist es z. B. möglich, dass bereits ausgeschiedene oder mit neuen Aufgaben betraute Mitarbeitende immer noch auf SAP-ERP-Systeme zugreifen können.

2.4. Fehlende SAP-Dokumentation und fehlende Notfallkonzepte

Gibt es keine Dokumentation für das SAP-ERP-System oder wird diese nicht gepflegt, lässt sich nicht mehr nachvollziehen, wie das SAP-ERP-System mit welchen Einstellungen aufgebaut wurde. Dadurch verzögern sich z. B. im Notfall die Wiederanlaufzeiten und geschäftskritische Prozesse fallen eventuell komplett aus. Diese Gefahr besteht auch, wenn es keine Notfallpläne gibt, die detailliert beschreiben, wie die Verantwortlichen im Ernstfall vorgehen sollen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.2 *SAP-ERP-System* 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	Fachabteilung, Notfallbeauftragte, Entwickelnde

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.4.2.A1 Sichere Konfiguration des SAP-ABAP-Stacks (B)

Der SAP-ABAP-Stack MUSS sicher konfiguriert werden. Dazu MÜSSEN die jeweiligen Profilparameter gesetzt werden, z. B. für die Passwortsicherheit, Authentisierung und Verschlüsselung. Auch MÜSSEN die Systemänderbarkeit und die Mandanten konfiguriert, das IMG-Customizing durchgeführt und die Betriebssystemkommandos abgesichert werden.

APP.4.2.A2 Sichere Konfiguration des SAP-JAVA-Stacks (B)

Der SAP-JAVA-Stack MUSS sicher konfiguriert werden, falls dieser eingesetzt wird. Dafür MÜSSEN andere Sicherheitsmechanismen und -konzepte erstellt werden als für den SAP-ABAP-Stack. Deshalb MÜSSEN Administrierende die Architektur des JAVA-Stacks kennen und wissen, wie er administriert wird. Zudem MÜSSEN nicht benötigte Dienste abgeschaltet, Standardinhalte entfernt, HTTP-Dienste geschützt und Zugriffe auf Administrationsschnittstellen eingeschränkt werden.

APP.4.2.A3 Netzsicherheit (B)

Um die Netzsicherheit zu gewährleisten, MÜSSEN entsprechende Konzepte unter Berücksichtigung des SAP-ERP-Systems erstellt und Einstellungen am System durchgeführt werden.

Weiterhin SOLLTEN der SAP-Router und SAP Web Dispatcher eingesetzt werden, um ein sicheres SAP-Netz zu implementieren und aufrechtzuerhalten.

Um Sicherheitslücken aufgrund von Fehlinterpretationen oder Missverständnissen zu vermeiden, MÜSSEN sich die Bereiche IT-Betrieb, Firewall-Betrieb, Portalbetrieb und SAP-Betrieb miteinander abstimmen.

APP.4.2.A4 Absicherung der ausgelieferten SAP-Standard-Konten (B)

Direkt nach der Installation eines SAP-ERP-Systems MÜSSEN die voreingestellten Passwörter der SAP-Standard-Konten geändert werden. Auch MÜSSEN die eingerichteten SAP-Standard-Konten mithilfe geeigneter Maßnahmen abgesichert werden. Bestimmte SAP-Standard-Konten DÜRFEN NICHT benutzt werden, z. B. für RFC-Verbindungen und Background-Jobs.

APP.4.2.A5 Konfiguration und Absicherung der SAP-Konten-Verwaltung (B)

Die SAP-Konten-Verwaltung für ABAP-Systeme MUSS sorgfältig und sicher administriert werden. Aktivitäten, wie Konten anlegen, ändern und löschen, Passwörter zurücksetzen und entsperren sowie Rollen und Profile zuordnen, MÜSSEN zu den Aufgaben der Konto-Administration gehören.

APP.4.2.A6 Erstellung und Umsetzung eines Konten- und Berechtigungskonzeptes (B) [Fachabteilung, Entwickelnde]

Für SAP-ERP-Systeme MUSS ein Konten- und Berechtigungskonzept ausgearbeitet und umgesetzt werden. Dabei MÜSSEN folgende Punkte berücksichtigt werden:

- Identitätsprinzip, Minimalprinzip, Stellenprinzip, Belegprinzip der Buchhaltung, Belegprinzip der Berechtigungsverwaltung, Funktionstrennungsprinzip (Segregation of Duties, SoD), Genehmigungsprinzip, Standardprinzip, Schriftformprinzip und Kontrollprinzip MÜSSEN berücksichtigt werden.
- Konto-, Berechtigungs- und gegebenenfalls Profiladministrierender MÜSSEN getrennte Verantwortlichkeiten und damit Berechtigungen haben.
- Vorgehensweisen im Rahmen der Berechtigungsadministration für *Rollen anlegen, ändern, löschen, transportieren und SU24 Vorschlagswerte transportieren* MÜSSEN definiert werden. Dabei SOLLTEN Berechtigungsrollen nur im Entwicklungssystem angelegt und gepflegt werden. Sie SOLLTEN mit Hilfe des Transport-Management-Systems (TMS) transportiert werden. Berechtigungen SOLLTEN in Berechtigungsrollen (PFCG-Rollen) angelegt, gespeichert und den Konten zugeordnet werden (rollenbasiertes Berechtigungskonzept). Da sich einzelne kritische Aktionen in den Rollen nicht immer vermeiden lassen, SOLLTEN sie von kompensierenden Kontrollen (mitigation controls) abgedeckt werden.
- Vorgehensweisen im Rahmen der Berechtigungsvergabe für *Konten und Berechtigungen beantragen, genehmigen, ändern und löschen* MÜSSEN definiert werden.
- Namenskonventionen für Konten-Kennungen und technische Rollennamen MÜSSEN definiert werden.
- Vorschlagswerte und Prüfkennzeichen SOLLTEN in der Transaktion SU24 gepflegt werden. Die Vorgehensweise dazu SOLLTE im Konten- und Berechtigungskonzept beschrieben sein.
- Gesetzliche und interne Rahmenbedingungen wie die Grundsätze ordnungsgemäßer Buchführung (GoB), das Handelsgesetzbuch (HGB) oder interne Vorgaben der Institution MÜSSEN berücksichtigt werden. Das Konten- und Berechtigungskonzept SOLLTE auch den Betrieb technischer Konten abdecken, also auch die Berechtigung von Hintergrund- und Schnittstellenkonten.

Es SOLLTEN geeignete Kontrollmechanismen angewandt werden, um SoD-Konfliktfreiheit von Rollen und die Vergabe von kritischen Berechtigungen an Konten zu überwachen.

Werden neben dem ABAP-Backend weitere Komponenten wie SAP HANA und SAP NetWeaver Gateway (für Fiori-Anwendungen) verwendet, MUSS das Design der Berechtigungen zwischen den Komponenten abgestimmt und synchronisiert werden.

APP.4.2.A7 Absicherung der SAP-Datenbanken (B)

Der Zugriff auf SAP-Datenbanken MUSS abgesichert werden. Administrierende SOLLTEN möglichst nur mit SAP-Tools auf die Datenbanken zugreifen können. Wird dazu Software von fremden

Institutionen benutzt, MÜSSEN zusätzliche Sicherheitsmaßnahmen umgesetzt werden. Es DARF dann kein Schema-Konto des SAP Systems für die Verbindung zur Datenbank genutzt werden. Außerdem MÜSSEN Standardpasswörter geändert und bestimmte Datenbanktabellen (z. B. USR* Tabellen) besonders geschützt werden.

APP.4.2.A8 Absicherung der SAP-RFC-Schnittstelle (B)

Zum Schutz der Remote-Function-Call (RFC)-Schnittstelle MÜSSEN RFC-Verbindungen, RFC-Berechtigungen und die RFC-Gateways sicher konfiguriert werden.

Es MÜSSEN für alle RFC-Verbindungen einheitliche Verwaltungsrichtlinien erstellt und umgesetzt werden. Dazu SOLLTEN die benötigten RFC-Verbindungen definiert und dokumentiert werden. Verbindungen mit hinterlegtem Passwort SOLLTEN nicht von niedriger privilegierten auf höher privilegierte Systeme (z. B. von *Dev* nach *Prod*) konfiguriert sein. Nicht mehr benutzte RFC-Verbindungen MÜSSEN gelöscht werden.

Alle RFC-Gateways MÜSSEN sicher administriert werden. Dazu MÜSSEN geeignete Profilparameter gesetzt werden, z. B. *gw/monitor, gw/reg_no_conn_info* und *snc/permit_insecure_start*. Alle Verbindungen über ein Gateway MÜSSEN unter dem Sicherheitsaspekt analysiert und bewertet werden. Außerdem MUSS die Protokollierung aktiv sein. Es MÜSSEN Zugriffssteuerungslisten (ACLs) definiert werden.

APP.4.2.A9 Absicherung und Überwachung des Message-Servers (B)

Der Message-Server MUSS durch geeignete Einstellungen in den Profilparametern abgesichert werden. Es MUSS unter anderem entschieden werden, ob für den internen Message-Server noch ACLs aufgebaut werden. Der Message-Server MUSS mithilfe von geeigneten Mechanismen überwacht werden, damit z. B. Systemausfälle des Message-Servers schnell erkannt werden.

APP.4.2.A10 ENTFALLEN (B)

Diese Anforderung ist entfallen.

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.4.2.A11 Sichere Installation eines SAP-ERP-Systems (S)

Bei der Installation eines SAP-ERP-Systems SOLLTEN aktuelle SAP-Sicherheitsleitfäden und -Dokumentationen berücksichtigt werden. Außerdem SOLLTEN die Sicherheitsrichtlinien der Institution eingehalten werden. Ebenso SOLLTE gewährleistet sein, dass das SAP-ERP-System auf einem abgesicherten Betriebssystem installiert wird.

APP.4.2.A12 SAP-Berechtigungsentwicklung (S) [Fachabteilung, Entwickelnde]

Die technischen Berechtigungen SOLLTEN aufgrund fachlicher Vorgaben entwickelt werden. Des Weiteren SOLLTEN SAP-Berechtigungen auf dem Entwicklungssystem der SAP-Landschaft angepasst oder neu erstellt werden. Das SOLLTE auch bei S/4HANA die Berechtigungsentwicklung auf HANA-Datenbanken mit einschließen. Hier SOLLTEN Repository-Rollen aufgebaut und transportiert werden. Datenbankprivilegien SOLLTEN NICHT direkt an Konten vergeben werden.

Bei Eigenentwicklungen für z. B. Transaktionen oder Berechtigungsobjekte SOLLTE die Transaktion SU24 gepflegt werden (Zuordnungen von Berechtigungsobjekten zu Transaktionen). Die Gesamtberechtigung * oder Intervalle in Objektausprägungen SOLLTEN vermieden werden.

Die Berechtigungsentwicklung SOLLTE im Rahmen eines Änderungsmanagements durchgeführt werden.

Es SOLLTE sichergestellt sein, dass das Produktivsystem ausreichend vor Berechtigungsänderungen geschützt ist und keine Entwicklerschlüssel vergeben werden. Das Qualitätssicherungssystem SOLLTE bei der Berechtigungsvergabe und ergänzenden Einstellungen analog zum Produktivsystem betrieben werden.

APP.4.2.A13 SAP-Passwortsicherheit (S)

Um eine sichere Anmeldung am SAP-ERP-System zu gewährleisten, SOLLTEN Profilparameter, Customizing-Schalter oder Sicherheitsrichtlinien geeignet eingestellt werden.

Die eingesetzten Hash-Algorithmen für die gespeicherten Hashwerte der Passwörter in einem SAP-ERP-System SOLLTEN den aktuellen Sicherheitsstandards entsprechen. Zugriffe auf Tabellen mit Hashwerten SOLLTEN eingeschränkt werden.

APP.4.2.A14 Identifizierung kritischer SAP-Berechtigungen (S) [Fachabteilung]

Der Umgang mit kritischen Berechtigungen SOLLTE streng kontrolliert werden. Es SOLLTE darauf geachtet werden, dass diese Berechtigungen, Rollen und Profile nur restriktiv vergeben werden. Dies SOLLTE auch für kritische Rollenkombinationen und additive Effekte wie z. B. Kreuzberechtigungen sichergestellt sein.

Kritische Berechtigungen SOLLTEN regelmäßig identifiziert, überprüft und bewertet werden. Die SAP-Profile *SAP_ALL* und *SAP_NEW** sowie das SAP-Berechtigungsobjekt *S_DEVELOP* (mit Änderungsberechtigungen *ACTVT 01* und *02*) SOLLTEN im Produktivsystem nicht vergeben werden. Notfall-Konten SOLLTEN von dieser Vorgabe ausgeschlossen sein.

APP.4.2.A15 Sichere Konfiguration des SAP-Routers (S)

Der SAP-Router SOLLTE den Zugang zum Netz regeln und die bestehende Firewall-Architektur zweckmäßig ergänzen. Auch SOLLTE er den Zugang zum SAP-ERP-System kontrollieren.

APP.4.2.A16 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows (S)

Das SAP-ERP-System SOLLTE NICHT auf einem Windows-Domaincontroller installiert werden. Die SAP-spezifischen Konten wie *<sid>adm* oder *SAPService <sid>* SOLLTEN abgesichert werden. Nach der Installation SOLLTE das Konto *<db><sid>* gesperrt werden.

Das Konto SAPService *<sid>* SOLLTE KEINE Rechte zur interaktiven Anmeldung besitzen. In Bezug auf diese Berechtigungen SOLLTEN die zum SAP-ERP-System dazugehörigen Systemressourcen wie Dateien, Prozesse und gemeinsam genutzte Speicher geschützt werden.

Die spezifischen Berechtigungen der vom SAP-ERP-System angelegten Konten *Guest, System, SAP system users = <sapsid>adm, SAPService<SAPSID>* und *Database users = <database-specific users>* und Benutzendengruppen SOLLTEN mithilfe geeigneter Einstellungen abgesichert werden.

APP.4.2.A17 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Unix (S)

Für die SAP-ERP-Systemverzeichnisse unter Unix SOLLTEN Zugriffsberechtigungen festgelegt werden. Auch SOLLTEN die Passwörter der systemspezifischen Konten *<sid>adm* und *<db><sid>* geändert werden. Nach der Installation SOLLTE das Konto *<db><sid>* gesperrt werden.

APP.4.2.A18 Abschaltung von unsicherer Kommunikation (S)

Die Kommunikation mit und zwischen SAP-ERP-Systemen SOLLTE mit SNC abgesichert werden. Sofern Datenbank und SAP-Applikationsserver auf verschiedenen Systemen betrieben werden, SOLLTE die Datenbankverbindung in geeigneter Weise verschlüsselt werden. Die internen Dienste des SAP-Applikationsservers SOLLTEN NUR mittels TLS miteinander kommunizieren.

APP.4.2.A19 Definition der Sicherheitsrichtlinien für Konten (S)

Für die jeweiligen Konten und Kontengruppen SOLLTEN spezifische Sicherheitsrichtlinien für Passwörter und Anmelderestriktionen erstellt werden. So SOLLTEN beispielsweise Konten mit kritischen Berechtigungen durch starke Passwortregeln abgesichert sein (Transaktion SECPOL). Die Sicherheitsrichtlinien SOLLTEN den Konten korrekt zugeordnet und regelmäßig überprüft werden.

APP.4.2.A20 Sichere SAP-GUI-Einstellungen (S)

Die SAP GUI SOLLTE auf allen Clients installiert und regelmäßig aktualisiert werden. Auch SOLLTEN SAP GUI ACLs aktiviert sowie angemessene Administrationsregeln verteilt und aktiviert werden.

APP.4.2.A21 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.2.A22 Schutz des Spools im SAP-ERP-System (S) [Entwickelnde]

Es SOLLTE sichergestellt sein, dass auf Daten der sequenziellen Datenverarbeitung wie Spool oder Druck nur eingeschränkt zugegriffen werden kann. Auch SOLLTE verhindert werden, dass unberechtigte Konten auf die vom SAP-Spoolsystem benutzte Datenablage TemSe zugreifen können. Die hierfür vergebenen Berechtigungen SOLLTEN regelmäßig überprüft werden.

APP.4.2.A23 Schutz der SAP-Hintergrundverarbeitung (S) [Entwickelnde]

Die SAP-Hintergrundverarbeitung SOLLTE vor unberechtigten Zugriffen geschützt werden. Dafür SOLLTEN für Batch-Jobs verschiedene System-Konten nach ihren Funktionsbereichen definiert und angelegt werden. Der so genannte Benutzertyp Dialog SOLLTE dafür grundsätzlich NICHT zugelassen werden.

APP.4.2.A24 Aktivierung und Absicherung des Internet Communication Frameworks (S)

Es SOLLTE darauf geachtet werden, dass nur notwendige ICF-Dienste aktiviert werden. Alle ICF-Dienste, die unter einem ICF-Objekt sind, SOLLTEN nur einzeln aktiviert werden. ICF-Berechtigungen SOLLTEN restriktiv vergeben werden. Die Kommunikation SOLLTE verschlüsselt erfolgen.

APP.4.2.A25 Sichere Konfiguration des SAP Web Dispatchers (S)

Der SAP Web Dispatcher SOLLTE nicht der erste Einstiegspunkt aus dem Internet zum SAP-ERP-System sein. Der SAP Web Dispatcher SOLLTE auf dem aktuellen Stand sein. Er SOLLTE sicher konfiguriert sein.

APP.4.2.A26 Schutz von selbstentwickeltem Code im SAP-ERP-System (S)

Es SOLLTE ein Custom-Code-Managementprozess definiert werden, damit selbstentwickelter Code ausgetauscht oder entfernt wird, falls er durch SAP-Standard-Code ersetzt werden kann oder er nicht mehr benutzt wird. Ferner SOLLTEN die Anforderungen aus der Richtlinie für die Entwicklung von ABAP-Programmen berücksichtigt werden.

APP.4.2.A27 Audit des SAP-ERP-Systems (S) [Fachabteilung]

Damit sichergestellt ist, dass alle internen und externen Richtlinien sowie Vorgaben eingehalten werden, SOLLTEN alle SAP-ERP-Systeme regelmäßig auditiert werden. Dafür SOLLTE der Security Optimization Service im SAP Solution Manager benutzt werden. Die Ergebnisse des Audits SOLLTEN ausgewertet und dokumentiert werden.

APP.4.2.A28 Erstellung eines Notfallkonzeptes (S) [Notfallbeauftragte]

Für SAP-ERP-Systeme SOLLTE ein Notfallkonzept erstellt und betrieben werden. Es SOLLTE die Geschäftsaktivitäten absichern und mit den Vorgaben aus dem Krisenmanagement oder dem

Business-Continuity-Management übereinstimmen. Im Notfallkonzept SOLLTEN folgende Punkte beschrieben und definiert werden:

- Detektion von und Reaktion auf Zwischenfälle,
- Datensicherungs- und Wiederherstellungskonzept sowie
- Notfalladministration.

Das Notfallkonzept SOLLTE regelmäßig aktualisiert werden.

APP.4.2.A29 Einrichten von Notfall-Konten (S)

Es SOLLTEN Notfall-Konten angelegt werden. Die eingerichteten Konten und Berechtigungen SOLLTEN stark kontrolliert und genau dokumentiert werden. Außerdem SOLLTEN alle von Notfall-Konten durchgeführten Aktivitäten protokolliert werden.

APP.4.2.A30 Implementierung eines kontinuierlichen Monitorings der Sicherheitseinstellungen (S)

Es SOLLTE ständig überwacht werden, ob alle Sicherheitseinstellungen des SAP-ERP-Systems korrekt sind. Außerdem SOLLTE überwacht werden, ob alle Patches und Updates ordnungsgemäß eingespielt wurden. Das SAP-Monitoring SOLLTE in die allgemeine Systemüberwachung der Institution integriert werden.

APP.4.2.A31 Konfiguration von SAP Single-Sign-On (S)

Sind mehrere SAP-ERP-Systeme vorhanden, SOLLTEN die Benutzenden auf die Systeme mit SAP Single-Sign-On (SAP SSO) zugreifen. Es SOLLTE in der Planungsphase entschieden werden, zwischen welchen SAP-ERP-Systemen der SSO-Mechanismus benutzt wird. Das SSO SOLLTE sicher konfiguriert und betrieben werden.

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.4.2.A32 Echtzeiterfassung und Alarmierung von irregulären Vorgängen (H)

Die wichtigsten Sicherheitsaufzeichnungsfunktionen der SAP-ERP-Systeme wie Security Audit Log oder System Log SOLLTEN kontinuierlich überwacht werden. Bei verdächtigen Vorgängen SOLLTEN automatisch die zuständigen Mitarbeitenden alarmiert werden. Um SAP-spezifische Sicherheitsvorfälle analysieren und Falschmeldungen von echten Sicherheitsvorfällen abgrenzen zu können, SOLLTEN entweder Mitarbeitende geschult oder entsprechende Serviceleistungen von Drittanbietenden genutzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das SAP Help Portal (https://www.help.sap.com/viewer/index) ist der zentrale Einstieg in die SAP Hilfe. Sie bietet zu vielfältigen Themen umfangreiche Informationen und Anleitungen. Im Folgenden wird eine Auswahl an Themen, die im Kontext SAP-ERP-Systeme interessant sind, aufgelistet:

- SAP Audit Management, https://help.sap.com/saphelp_fra110/helpdata/de/ab/ce1b52bd543c3ae10000000a441470/fram

eset.htm und
https://help.sap.com/saphel_erp60_sp/helpdata/de/f9/558f40f3b19920e10000000a1550b0/content.htm

- Benutzerverwaltung mit AS Java,
https://help.sap.com/saphelp_nw73/helpdata/de/45/b90177cf2252f8e10000000a1553f7/content.htm?no_cache=true
- Zentrale Benutzerverwaltung (ZBV), https://help.sap.com/doc/erp2005_ehp_07/6.07/de-DE/8d/270bea613d2443bad6ce0524f08ca0/frameset.htm

Detaillierte Best-Practice-Empfehlungen für die Prüfungen von SAP-ERP-Systemen, bietet der Prüfleitfaden SAP ERP 6.0: Best Practice - Empfehlungen der Deutschsprachigen SAP Anwendergruppe e. V. (DSAG).

Bundesamt
für Sicherheit in der
Informationstechnik

APP.4.3 Relationale Datenbanken

1. Beschreibung

1.1. Einleitung

Datenbanksysteme (DBS) sind ein oft genutztes Hilfsmittel, um IT-gestützt große Datensammlungen zu organisieren, zu erzeugen, zu verändern und zu verwalten. Ein DBS besteht aus dem so genannten Datenbankmanagementsystem (DBMS) und einer oder mehreren Datenbanken. Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die dauerhaft im Datenbanksystem abgelegt werden. Da Datenbanksysteme oft eine zentrale Bedeutung in einer IT-Infrastruktur einnehmen, ergeben sich an sie wesentliche Sicherheitsanforderungen. Meist sind Kernprozesse einer Institution von den Informationen aus den Datenbanken abhängig. Dadurch ergeben sich entsprechende Verfügbarkeitsanforderungen. Zusätzlich bestehen oft hohe Anforderungen an die Vertraulichkeit und Integrität der in den Datenbanken gespeicherten Informationen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, relationale Datenbanksysteme sicher betreiben zu können sowie die Informationen, die in Datenbanken verarbeitet und gespeichert werden, angemessen zu schützen. Dazu werden Anforderungen beschrieben, mit denen sich Datenbanksysteme sicher planen, umsetzen und betreiben lassen und durch die Gefährdungen reduziert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein APP.4.3 *Relationale Datenbanken* ist auf jedes relationale Datenbanksystem einmal anzuwenden.

In diesem Baustein werden Anforderungen an relationale Datenbanksysteme beschrieben. Sicherheitsanforderungen an nicht-relationale Datenbanksysteme sind nicht Gegenstand des vorliegenden Bausteins.

Um die Informationen in den Datenbanken durchgängig zu schützen, sollten bereits in der Anwendungsentwicklung Sicherheitsanforderungen an den Aufbau der Datenbanktabellen und den Zugriff auf die Datenbank beachtet werden. Anforderungen zu diesen Themen werden jedoch nicht in diesem Baustein aufgeführt.

Ebenso geht der Baustein nicht auf Gefährdungen und Anforderungen ein, die das Betriebssystem und die Hardware betreffen, auf denen das Datenbanksystem installiert ist. Aspekte dazu finden sich in den

entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme*, z. B. SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server*.

Relationale Datenbanksysteme sollten grundsätzlich im Rahmen der Bausteine OPR.4 *Identitäts- und Berechtigungsmanagement,* OPS.1.1.3 *Patch- und Änderungsmanagement*, CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

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.4.3 *Relationale Datenbanken* von besonderer Bedeutung.

2.1. Unzureichende Dimensionierung der Systemressourcen

Verfügt die Hardware eines Datenbanksystems nicht über genügend Systemressourcen, kann die Datenbank ganz ausfallen oder fehlerhaft arbeiten. Dadurch können beispielsweise Daten nicht gespeichert werden. Auch können zu Stoßzeiten die Ressourcen stark ausgelastet werden. Dadurch kann sich die Performance verschlechtern. Dies wiederum kann dazu führen, dass Anwendungen nicht oder nicht fehlerfrei ausgeführt werden.

2.2. Aktivierte Standard-Konten

Bei der Erstinstallation bzw. im Auslieferungszustand eines Datenbankmanagementsystems sind Standard-Konten (Konten der Benutzenden und Administrierenden) häufig nicht oder nur mit Passwörtern gesichert, die öffentlich bekannt sind. Dadurch kann es passieren, dass diese Konten missbräuchlich genutzt werden. Beispielsweise können sich Angreifende mit den öffentlich bekannten Anmeldedaten am Datenbankmanagementsystem als Benutzende oder sogar als Administrierende anmelden. Danach können sie die Konfiguration oder die gespeicherten Daten auslesen, manipulieren oder löschen.

2.3. Unverschlüsselte Datenbankanbindung

In der Standardkonfiguration verbinden sich viele Datenbankmanagementsysteme unverschlüsselt mit den Anwendungen. Wird zwischen Anwendungen und Datenbankmanagementsystem unverschlüsselt kommuniziert, können übertragene Daten und Zugangsinformationen mitgelesen oder auf dem Transportweg manipuliert werden.

2.4. Datenverlust in der Datenbank

Durch Hardware- oder Softwarefehler sowie durch menschliches Versagen können Daten in der Datenbank verloren gehen. Da in Datenbanken meist wichtige Informationen für Anwendungen gespeichert sind, können Dienste ausfallen oder ganze Produktionsprozesse stillstehen.

2.5. Integritätsverlust der gespeicherten Daten

Durch falsch konfigurierte Datenbanken, Softwarefehler oder manipulierte Daten kann die Integrität der Informationen in der Datenbank verletzt werden. Wird dies nicht oder erst spät bemerkt, können Kernprozesse der Institution stark beeinträchtigt werden. Werden beispielsweise die Integritätsbeziehungen (referenzielle Integrität) zwischen den Tabellen nicht korrekt definiert, kann dies dazu führen, dass die Daten in der Datenbank fehlerhaft sind. Wird dieser Fehler erst im

Produktivbetrieb oder gar nicht bemerkt, müssen nicht nur die inkonsistenten Daten aufwändig bereinigt und rekonstruiert werden. Es kann mit der Zeit auch ein großer Schaden entstanden sein, beispielsweise wenn es sich um kritische Daten, zum Beispiel steuerrelevante Daten, Rechnungsdaten oder gar um Steuerungsdaten für ganze Produktionssysteme handelt.

2.6. SQL-Injections

Eine häufige Angriffsmethode auf Datenbanksysteme sind SQL-Injections. Greift eine Anwendung auf die Daten einer SQL-Datenbank zu, so werden Befehle in Form von SQL-Anweisungen an das DBMS übermittelt. Werden Eingabedaten innerhalb der Anwendung unzureichend validiert, können Angreifende eigene SQL-Befehle in die Anwendung einschleusen, die dann mit der Berechtigung des Dienstkontos der Anwendung bearbeitet werden. Angreifende können so Daten lesen, manipulieren, löschen, neue Daten hinzufügen oder auch Systembefehle aufrufen. Obwohl SQL-Injections primär die Anwendungen im Frontend betreffen, wirken sie sich auch erheblich auf das Datenbanksystem selbst und die damit verbundene Infrastruktur aus.

2.7. Unsichere Konfiguration des Datenbankmanagementsystems

Häufig sind in der Standardkonfiguration des Datenbankmanagementsystems nicht benötigte Funktionen aktiviert, die es bei einem potenziellen Angriff erleichtern, Informationen aus der Datenbank auszulesen oder zu manipulieren. Beispielsweise können sich Angreifende aufgrund einer unveränderten Standardinstallation mit einer von der Institution nicht benutzten Programmierschnittstelle verbinden, um das DBMS zu administrieren, ohne sich dafür authentifizieren zu müssen. Dadurch können sie unerlaubt auf die Datenbanken der Institution zugreifen.

2.8. Malware und unsichere Datenbank-Skripte

Bei vielen Datenbankmanagementsystemen ist es möglich, bestimmte Aktionen über Skripte zu automatisieren, die im Kontext der Datenbank ausgeführt werden, z. B. mithilfe der Procedural Language/Structured Query Language (PL/SQL). Dazu gehören unter anderem auch sogenannte Datenbanktrigger. Werden diese jedoch von den Zuständigen ungeprüft benutzt, könnten die Datenbankskripte nicht den Anforderungen an die Softwareentwicklung der Institution genügen.

Ebenfalls können bei Angriffen Kernfunktionen einer Datenbank, wie z. B. Data Dictionary Tables manipuliert werden, beispielsweise mithilfe von Schadprogrammen oder Datenbank-Skripten. Diese Art von Angriffen ist nur schwer zu entdecken. Qualitätsmängel in diesen Skripten und Malware können sowohl die Vertraulichkeit als auch die Integrität und die Verfügbarkeit der in den Datenbanken abgelegten Daten gefährden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.3 *Relationale Datenbanken* 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, Entwickelnde

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.4.3.A1 Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für Datenbanksysteme erstellt werden. Darin MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Datenbanksysteme sicher betrieben werden sollen. Die Richtlinie MUSS allen im Bereich Datenbanksysteme zuständigen Mitarbeitenden bekannt sein. Sie MUSS grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem oder der ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

APP.4.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A3 Basishärtung des Datenbankmanagementsystems (B)

Das Datenbankmanagementsystem MUSS gehärtet werden. Hierfür MUSS eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden. Passwörter DÜRFEN NICHT im Klartext gespeichert werden. Die Basishärtung MUSS regelmäßig überprüft und, falls erforderlich, angepasst werden.

APP.4.3.A4 Geregeltes Anlegen neuer Datenbanken (B)

Neue Datenbanken MÜSSEN nach einem definierten Prozess angelegt werden. Wenn eine neue Datenbank angelegt wird, MÜSSEN Grundinformationen zur Datenbank nachvollziehbar dokumentiert werden.

APP.4.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A7 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A8 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A9 Datensicherung eines Datenbanksystems (B)

Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. Auch bevor eine Datenbank neu erzeugt wird, MUSS das Datenbanksystem gesichert werden. Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden.

Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind. Wenn die Datensicherung die verfügbaren Kapazitäten übersteigt, SOLLTE ein erweitertes Konzept erstellt

werden, um die Datenbank zu sichern, z. B. eine inkrementelle Sicherung. Abhängig vom Schutzbedarf der Daten SOLLTEN die Wiederherstellungsparameter vorgegeben werden (siehe CON.3 *Datensicherungskonzept)*.

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.4.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.3.A11 Ausreichende Dimensionierung der Hardware (S) [Fachverantwortliche]

Datenbankmanagementsysteme SOLLTEN auf ausreichend dimensionierter Hardware installiert werden. Die Hardware SOLLTE über genügend Reserven verfügen, um auch eventuell steigenden Anforderungen gerecht zu werden. Zeichnen sich trotzdem während des Betriebs Ressourcenengpässe ab, SOLLTEN diese frühzeitig behoben werden. Wenn die Hardware dimensioniert wird, SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.

APP.4.3.A12 Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen (S)

Für alle eingesetzten Datenbankmanagementsysteme SOLLTE ein einheitlicher Konfigurationsstandard definiert werden. Alle Datenbankmanagementsysteme SOLLTEN nach diesem Standard konfiguriert und einheitlich betrieben werden. Falls es bei einer Installation notwendig ist, vom Konfigurationsstandard abzuweichen, SOLLTEN alle Schritte von dem oder der ISB freigegeben und nachvollziehbar dokumentiert werden. Der Konfigurationsstandard SOLLTE regelmäßig überprüft und, falls erforderlich, angepasst werden.

APP.4.3.A13 Restriktive Handhabung von Datenbank-Links (S)

Es SOLLTE sichergestellt sein, dass nur Zuständige dazu berechtigt sind, Datenbank-Links (DB-Links) anzulegen. Werden solche Links angelegt, MÜSSEN so genannte Private DB-Links vor Public DB-Links bevorzugt angelegt werden. Alle von den Zuständigen angelegten DB-Links SOLLTEN dokumentiert und regelmäßig überprüft werden. Zudem SOLLTEN DB-Links mitberücksichtigt werden, wenn das Datenbanksystem gesichert wird (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*).

APP.4.3.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.3.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.3.A16 Verschlüsselung der Datenbankanbindung (S)

Das Datenbankmanagementsystem SOLLTE so konfiguriert werden, dass Datenbankverbindungen immer verschlüsselt werden. Die dazu eingesetzten kryptografischen Verfahren und Protokolle SOLLTEN den internen Vorgaben der Institution entsprechen (siehe CON.1 *Kryptokonzept*).

APP.4.3.A17 Datenübernahme oder Migration (S) [Fachverantwortliche]

Es SOLLTE vorab definiert werden, wie initial oder regelmäßig Daten in eine Datenbank übernommen werden sollen. Nachdem Daten übernommen wurden, SOLLTE geprüft werden, ob sie vollständig und unverändert sind.

APP.4.3.A18 Überwachung des Datenbankmanagementsystems (S)

Die für den sicheren Betrieb kritischen Parameter, Ereignisse und Betriebszustände des Datenbankmanagementsystems SOLLTEN definiert werden. Diese SOLLTEN mithilfe eines Monitoring-Systems überwacht werden. Für alle kritischen Parameter, Ereignisse und Betriebszustände SOLLTEN Schwellwerte festgelegt werden. Wenn diese Werte überschritten werden, MUSS geeignet reagiert werden. Hierbei SOLLTEN die zuständigen Mitarbeitenden alarmiert werden. Anwendungsspezifische Parameter, Ereignisse, Betriebszustände und deren Schwellwerte SOLLTEN mit den Zuständigen für die Fachanwendungen abgestimmt werden.

APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten (S) [Entwickelnde]

Werden Datenbank-Skripte entwickelt, SOLLTEN dafür verpflichtende Qualitätskriterien definiert werden (siehe CON.8 *Software-Entwicklung*). Datenbank-Skripte SOLLTEN ausführlichen Funktionstests auf gesonderten Testsystemen unterzogen werden, bevor sie produktiv eingesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A20 Regelmäßige Audits (S)

Bei allen Komponenten des Datenbanksystems SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Dabei SOLLTE geprüft werden, ob der dokumentierte Stand dem Ist-Zustand entspricht und ob die Konfiguration des Datenbankmanagementsystems der dokumentierten Standardkonfiguration entspricht. Zudem SOLLTE geprüft werden, ob alle Datenbank-Skripte benötigt werden. Auch SOLLTE geprüft werden, ob sie dem Qualitätsstandard der Institution genügen. Zusätzlich SOLLTEN die Protokolldateien des Datenbanksystems und des Betriebssystems nach Auffälligkeiten untersucht werden (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*). Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert sein. Sie SOLLTEN mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

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.4.3.A21 Einsatz von Datenbank Security Tools (H)

Es SOLLTEN Informationssicherheitsprodukte für Datenbanken eingesetzt werden. Die eingesetzten Produkte SOLLTEN folgende Funktionen bereitstellen:

- Erstellung einer Übersicht über alle Datenbanksysteme,
- erweiterte Konfigurationsmöglichkeiten und Rechtemanagement der Datenbanken,
- Erkennung und Unterbindung von möglichen Angriffen (z. B. Brute Force Angriffe auf Konten, SQL-Injection) und
- Auditfunktionen (z. B. Überprüfung von Konfigurationsvorgaben).

APP.4.3.A22 Notfallvorsorge (H)

Für das Datenbankmanagementsystem SOLLTE ein Notfallplan erstellt werden, der festlegt, wie ein Notbetrieb realisiert werden kann. Die für den Notfallplan notwendigen Ressourcen SOLLTEN ermittelt werden. Zusätzlich SOLLTE der Notfallplan definieren, wie aus dem Notbetrieb der Regelbetrieb wiederhergestellt werden kann. Der Notfallplan SOLLTE die nötigen Meldewege, Reaktionswege, Ressourcen und Reaktionszeiten der Fachverantwortlichen festlegen. Auf Basis eines Koordinationsplans zum Wiederanlauf SOLLTEN alle von der Datenbank abhängigen IT-Systeme vorab ermittelt und berücksichtigt werden.

APP.4.3.A23 Archivierung (H)

Ist es erforderlich, Daten eines Datenbanksystems zu archivieren, SOLLTE ein entsprechendes Archivierungskonzept erstellt werden. Es SOLLTE sichergestellt sein, dass die Datenbestände zu einem späteren Zeitpunkt wieder vollständig und konsistent verfügbar sind.

Im Archivierungskonzept SOLLTEN sowohl die Intervalle der Archivierung als auch die Vorhaltefristen der archivierten Daten festgelegt werden. Zusätzlich SOLLTE dokumentiert werden, mit welcher Technik die Datenbanken archiviert wurden. Mit den archivierten Daten SOLLTEN regelmäßig Wiederherstellungstests durchgeführt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A24 Datenverschlüsselung in der Datenbank (H)

Die Daten in den Datenbanken SOLLTEN verschlüsselt werden. Dabei SOLLTEN vorher unter anderem folgende Faktoren betrachtet werden:

- Einfluss auf die Performance,
- Schlüsselverwaltungsprozesse und -verfahren, einschließlich separater Schlüsselaufbewahrung und -sicherung,
- Einfluss auf Backup-Recovery-Konzepte,
- funktionale Auswirkungen auf die Datenbank, beispielsweise Sortiermöglichkeiten.

APP.4.3.A25 Sicherheitsprüfungen von Datenbanksystemen (H)

Datenbanksysteme SOLLTEN regelmäßig mithilfe von Sicherheitsprüfungen kontrolliert werden. Bei den Sicherheitsprüfungen SOLLTEN die systemischen und spezifischen Aspekte des herstellenden Unternehmens der eingesetzten Datenbank-Infrastruktur (z. B. Verzeichnisdienste) sowie des eingesetzten Datenbankmanagementsystems betrachtet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat im Rahmen der Allianz für Cybersicherheit zum Themenfeld Datenbanksicherheit folgende Partnerbeiträge veröffentlicht:

- Oracle: Datenbank-Sicherheit - Grundüberlegungen
- McAfee: Datenbanksicherheit in Virtualisierungs- und Cloud-Computing-Umgebungen

Die Deutsche Telekom Gruppe hat im Rahmen ihres Privacy and Security Assessment Verfahrens (PSA-Verfahren) das Dokument „Sicherheitsanforderung Datenbanksysteme“zum Themenfeld Datenbanken veröffentlicht.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel BA2.3 Protection of Databases Vorgaben für die Absicherung von relationalen Datenbanksystemen.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.4.4 Kubernetes

1. Beschreibung

1.1. Einleitung

Kubernetes hat sich als De-Facto-Standard für die Orchestrierung von Containern in der Public und Private Cloud etabliert. Auch für IoT und andere Anwendungsfälle ist Kubernetes im Einsatz, mit K3S gibt es beispielsweise eine Edition, die für sehr kleine Server wie Einplatinencomputer gedacht ist. Auch der sogenannte Cloud Native Stack, der aus vielen verschiedenen Komponenten besteht, baut auf dem von Kubernetes etablierten Standard auf.

Der Begriff *Container* bezeichnet eine Technik, bei der ein Host-System Anwendungen parallel in separierten Umgebungen ausführt (Operating System Level Virtualization). In den meisten Fällen erfolgt die Überwachung, das Starten und Beenden und die weitere Verwaltung der Container durch eine Verwaltungssoftware, die somit die sogenannte *Orchestrierung* übernimmt. Kubernetes fasst dabei einen oder mehrere zusammengehörige Container in einem *Pod* zusammen. Da der Fokus des Bausteins auf Kubernetes liegt, wird im Weiteren nur von Pods und nicht von einzelnen Containern gesprochen. Die Orchestrierung erfolgt dabei zumeist in Gruppen von gemeinsam verwalteten Kubernetes-Nodes in einem oder mehreren sogenannten *Clustern*.

Um die Orchestrierung von Pods zu betreiben und diese zu verwalten, haben sich mehrere Produkte etabliert, die es erlauben, auch sehr große Umgebungen zu bedienen. In ihrem Kern setzen allerdings alle auf Kubernetes auf. Bei der Betrachtung ist zwischen der *Runtime*, die die Prozesse auf den Kubernetes-Nodes betreibt, und der *Orchestrierung*, die die Runtimes auf mehreren Kubernetes-Nodes steuert, zu unterscheiden.

Zusätzlich zu diesen beiden zentralen Komponenten besteht der Betrieb von Kubernetes in den meisten Fällen noch aus einer spezialisierten Infrastruktur, zu der z. B. Registries, Code-Versionierung und -Speicherung, Automatisierungswerkzeuge, Verwaltungsserver, Speichersysteme oder virtuelle Netze gehören.

Die folgenden Begriffe werden im Baustein in dieser Bedeutung verwendet:

- *Anwendung* bezeichnet eine Zusammenstellung mehrerer Programme, die gemeinsam eine Aufgabe erfüllen
- *Cluster* sind Betriebsumgebungen für Container mit mehreren Nodes
- *Container* sind aus einem Image gestartete Prozesse, die innerhalb von Betriebssystem-Namespaces laufen

- *Container Network Interface (CNI)* bezeichnet die Schnittstelle zur Verwaltung der virtuellen Netze im Cluster
- *Container Storage Interface* (CSI) bezeichnet die Schnittstelle zu den zumeist externen Speichersystemen, die Kubernetes den Pods bereitstellen kann
- *Control Plane* bezeichnet alle für die Verwaltung, also Orchestrierung der Nodes, Runtimes und Cluster eingesetzten Anwendungen
- *Images* sind alle der Open Container Initiative (OCI) entsprechenden Software-Pakete, diese umfassen sowohl Basis-Images für eigene Images als auch solche Images, die unverändert im Einsatz sind
- *Node* bezeichnet einen Server, der für den Betrieb der Runtime installiert und optimiert ist
- *Pod* bezeichnet eine Sammlung mehrerer Container, die innerhalb der gleichen Betriebssystem-Namespaces laufen
- *Registry* ist der Oberbegriff für die Code-Verwaltung und die Speicherung der Images
- *Runtime* bezeichnet die Software, die die Software im Image als Container startet

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die in Kubernetes-Clustern verarbeitet, angeboten oder darüber übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein APP.4.4 *Kubernetes* ist immer zusammen mit dem Baustein SYS.1.6 *Containerisierung* anzuwenden. Dabei ist es bezogen auf den Fokus des vorliegenden Bausteins nicht relevant, welche Container-Runtime im Einsatz ist oder welche zusätzlichen Anwendungen Teil der Control Plane sind.

Der Baustein enthält grundsätzliche Anforderungen zur Einrichtung, zum Betrieb und zur Orchestrierung mit Kubernetes sowie zur spezialisierten Infrastruktur, die zum Betrieb notwendig ist. Letzteres beinhaltet Registries, CSI/CNI, Nodes und Automatisierungssoftware, soweit sie direkt mit dem Cluster interagieren. Die Anforderungen für diese Anwendungen beziehen sich zumeist auf die Schnittstellen, enthalten aber auch Anforderungen, die den Betrieb dieser Anwendungen betreffen, sofern sie direkt die Sicherheit des Clusters berühren. Weitere im Kubernetes-Umfeld übliche Dienste, wie z. B. Automatisierung für CI/CD-Pipelines und Codeverwaltung in z. B. Git, behandelt der Baustein nicht in der Tiefe.

Der Baustein modelliert umfassend einen Cluster. Die Anwendungen der Control Plane, Dienste zur Automatisierung und die Nodes, sind hier als eine Gruppe zu sehen und zu behandeln.

Sicherheitsanforderungen für die in Kubernetes-Clustern betriebenen Dienste, wie z. B. Webserver (APP.3.2 *Webserver*) oder E-Mail-Server (siehe APP.5.3 *Allgemeiner E-Mail-Client und -Server*), sind Gegenstand eigener Bausteine.

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.4.4 *Kubernetes* von besonderer Bedeutung.

2.1. Mangelhafte Authentisierung und Autorisierung in der Control Plane

Um Runtimes, Nodes und auch Kubernetes selbst zu verwalten, benötigen sowohl Administrierende als auch die toolgestützte Bereitstellung administrative Zugänge. Diese Zugänge sind entweder als Unix-Sockets oder Netzports ausgeführt. Mechanismen zur Authentisierung und Verschlüsselung der administrativen Zugänge sind häufig vorhanden, aber nicht bei allen Produkten standardmäßig aktiviert.

Wenn Unbefugte auf das Datennetz oder auf die Nodes zugreifen, können sie über ungeschützte administrative Zugänge Befehle ausführen, die der Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten Daten schaden können.

2.2. Vertraulichkeitsverlust von Zugangsdaten

Oft benötigen Pods Zugangsdaten (Access Token) für Kubernetes. Über einen Angriff auf den Pod können diese Zugangsdaten in unbefugte Hände gelangen. Mit diesen Zugangsdaten ist es bei Angriffen möglich, mit der Control Plane authentifiziert zu interagieren und, sofern die Berechtigungen ausreichen, auch Veränderungen an der Orchestrierung vorzunehmen.

2.3. Ressourcenkonflikte auf Nodes

Einzelne Pods können den Node oder auch die Orchestrierung überlasten und so die Verfügbarkeit aller anderen Pods auf dem Node oder auch den Betrieb des Nodes selbst gefährden.

2.4. Unautorisierte Änderungen an Clustern

Die Automatisierung mit CI/CD und die daraus folgende Notwendigkeit, den Werkzeugen privilegierte Zugangsberechtigungen zu erteilen, birgt das Risiko, dass nicht autorisierte Änderungen an Clustern erfolgen. So kann z. B. eine neue Version einer Anwendung auf dem Cluster aufgebracht werden, die nicht ausreichend getestet ist oder die den Freigabeprozess nicht durchlaufen hat. Auch ist es bei Fehlern in den Berechtigungen auf der CI/CD-Umgebung möglich, dass Schadsoftware in die Cluster eindringen und dort Daten auslesen, löschen oder verändern kann.

2.5. Unberechtigte Kommunikation

Alle Pods in einem Cluster sind grundsätzlich in der Lage, miteinander, mit den Nodes im eigenen Cluster sowie beliebigen anderen IT-Systemen zu kommunizieren. Sofern diese Kommunikation nicht eingeschränkt ist, kann dies ausgenutzt werden, um z. B. die Control Plane, andere Pods oder die Nodes anzugreifen.

Auch besteht die Gefahr, dass Pods im Cluster unerwünscht von außen erreichbar sind. So kann ein Angriff gegen Dienste, die eigentlich nur innerhalb des Clusters erreichbar sein sollten, von außen erfolgen. Diese Gefährdung wird durch die geringere Aufmerksamkeit verschlimmert, die internen Diensten oft entgegengebracht wird. Wird z. B. eine Verwundbarkeit auf einem nur intern eingesetzten Dienst toleriert und ist dieser auch von außen erreichbar, gefährdet dies den gesamten Cluster erheblich.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.4 *Kubernetes* 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	Keine

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.4.4.A1 Planung der Separierung der Anwendungen (B)

Vor der Inbetriebnahme MUSS geplant werden, wie die in den Pods betriebenen Anwendungen und deren unterschiedlichen Test- und Produktions-Betriebsumgebungen separiert werden. Auf Basis des Schutzbedarfs der Anwendungen MUSS festgelegt werden, welche Architektur der Namespaces, Meta-Tags, Cluster und Netze angemessen auf die Risiken eingeht und ob auch virtualisierte Server und Netze zum Einsatz kommen sollen.

Die Planung MUSS Regelungen zu Netz-, CPU- und Festspeicherseparierung enthalten. Die Separierung SOLLTE auch das Netzzonenkonzept und den Schutzbedarf beachten und auf diese abgestimmt sein.

Anwendungen SOLLTEN jeweils in einem eigenen Kubernetes-Namespace laufen, der alle Programme der Anwendung umfasst. Nur Anwendungen mit ähnlichem Schutzbedarf und ähnlichen möglichen Angriffsvektoren SOLLTEN einen Kubernetes-Cluster teilen.

APP.4.4.A2 Planung der Automatisierung mit CI/CD (B)

Wenn eine Automatisierung des Betriebs von Anwendungen in Kubernetes mithilfe von CI/CD stattfindet, DARF diese NUR nach einer geeigneten Planung erfolgen. Die Planung MUSS den gesamten Lebenszyklus von Inbetrieb- bis Außerbetriebnahme inklusive Entwicklung, Tests, Betrieb, Überwachung und Updates umfassen. Das Rollen- und Rechtekonzept sowie die Absicherung von Kubernetes Secrets MÜSSEN Teil der Planung sein.

APP.4.4.A3 Identitäts- und Berechtigungsmanagement bei Kubernetes (B)

Kubernetes und alle anderen Anwendungen der Control Plane MÜSSEN jede Aktion eines Benutzenden oder, im automatisierten Betrieb, einer entsprechenden Software authentifizieren und autorisieren, unabhängig davon, ob die Aktionen über einen Client, eine Weboberfläche oder über eine entsprechende Schnittstelle (API) erfolgt. Administrative Handlungen DÜRFEN NICHT anonym erfolgen.

Benutzende DÜRFEN NUR die unbedingt notwendigen Rechte erhalten. Berechtigungen ohne Einschränkungen MÜSSEN sehr restriktiv vergeben werden.

Nur ein kleiner Kreis von Personen SOLLTE berechtigt sein, Prozesse der Automatisierung zu definieren. Nur ausgewählte Administrierende SOLLTEN in Kubernetes das Recht erhalten, Freigaben für Festspeicher (Persistent Volumes) anzulegen oder zu ändern.

APP.4.4.A4 Separierung von Pods (B)

Der Betriebssystem-Kernel der Nodes MUSS über Isolationsmechanismen zur Beschränkung von Sichtbarkeit und Ressourcennutzung der Pods untereinander verfügen (vergleiche Linux Namespaces und cgroups). Die Trennung MUSS dabei mindestens IDs von Prozessen sowie Benutzenden, Inter-Prozess-Kommunikation, Dateisystem und Netz inklusive Hostname umfassen.

APP.4.4.A5 Datensicherung im Cluster (B)

Es MUSS eine Datensicherung des Clusters erfolgen. Die Datensicherung MUSS umfassen:

- Festspeicher (Persistent Volumes),
- Konfigurationsdateien von Kubernetes und den weiteren Programmen der Control Plane,
- den aktuellen Zustand des Kubernetes-Clusters inklusive der Erweiterungen,
- Datenbanken der Konfiguration, namentlich hier *etcd*,
- alle Infrastrukturanwendungen, die zum Betrieb des Clusters und der darin befindlichen Dienste notwendig sind und
- die Datenhaltung der Code und Image Registries.

Es SOLLTEN auch Snapshots für den Betrieb der Anwendungen betrachtet werden. Snapshots DÜRFEN die Datensicherung NICHT ersetzen.

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.4.4.A6 Initialisierung von Pods (S)

Sofern im Pod zum Start eine Initialisierung z. B. einer Anwendung erfolgt, SOLLTE diese in einem eigenen Init-Container stattfinden. Es SOLLTE sichergestellt sein, dass die Initialisierung alle bereits laufenden Prozesse beendet. Kubernetes SOLLTE nur bei erfolgreicher Initialisierung die weiteren Container starten.

APP.4.4.A7 Separierung der Netze bei Kubernetes (S)

Die Netze für die Administration der Nodes, der Control Plane sowie die einzelnen Netze der Anwendungsdienste SOLLTEN separiert werden.

Es SOLLTEN NUR die für den Betrieb notwendigen Netzports der Pods in die dafür vorgesehenen Netze freigegeben werden. Bei mehreren Anwendungen auf einem Kubernetes-Cluster SOLLTEN zunächst alle Netzverbindungen zwischen den Kubernetes-Namespaces untersagt und nur benötigte Netzverbindungen gestattet sein (Whitelisting). Die zur Administration der Nodes, der Runtime und von Kubernetes inklusive seiner Erweiterungen notwendigen Netzports SOLLTEN NUR aus dem Administrationsnetz und von Pods, die diese benötigen, erreichbar sein.

Nur ausgewählte Administrierende SOLLTEN in Kubernetes berechtigt sein, das CNI zu verwalten und Regeln für das Netz anzulegen oder zu ändern.

APP.4.4.A8 Absicherung von Konfigurationsdateien bei Kubernetes (S)

Die Konfigurationsdateien des Kubernetes-Clusters, inklusive aller Erweiterungen und Anwendungen, SOLLTEN versioniert und annotiert werden.

Zugangsrechte auf die Verwaltungssoftware der Konfigurationsdateien SOLLTEN minimal vergeben werden. Zugriffsrechte für lesenden und schreibenden Zugriff auf die Konfigurationsdateien der Control Plane SOLLTEN besonders sorgfältig vergeben und eingeschränkt sein.

APP.4.4.A9 Nutzung von Kubernetes Service-Accounts (S)

Pods SOLLTEN NICHT den "default"-Service-Account nutzen. Dem "default"-Service-Account SOLLTEN keine Rechte eingeräumt werden. Pods für unterschiedliche Anwendungen SOLLTEN jeweils unter eigenen Service-Accounts laufen. Berechtigungen für die Service-Accounts der Pods der Anwendungen SOLLTEN auf die unbedingt notwendigen Rechte beschränkt werden.

Pods, die keinen Service-Account benötigen, SOLLTEN diesen nicht einsehen können und keinen Zugriff auf entsprechende Token haben.

Nur Pods der Control Plane und Pods, die diese unbedingt benötigen, SOLLTEN privilegierte Service-Accounts nutzen.

Programme der Automatisierung SOLLTEN jeweils eigene Token erhalten, auch wenn sie aufgrund ähnlicher Aufgaben einen gemeinsamen Service-Account nutzen.

APP.4.4.A10 Absicherung von Prozessen der Automatisierung (S)

Alle Prozesse der Automatisierungssoftware, wie CI/CD und deren Pipelines, SOLLTEN nur mit unbedingt notwendigen Rechten arbeiten. Wenn unterschiedliche Gruppen von Benutzenden die Konfiguration über die Automatisierungssoftware verändern oder Pods starten können, SOLLTE dies für jede Gruppe durch eigene Prozesse durchgeführt werden, die nur die für die jeweilige Gruppe notwendigen Rechte besitzen.

APP.4.4.A11 Überwachung der Container (S)

In Pods SOLLTE jeder Container einen Health Check für den Start und den Betrieb („readiness“ und „liveness“) definieren. Diese Checks SOLLTEN Auskunft über die Verfügbarkeit der im Pod ausgeführten Software geben. Die Checks SOLLTEN fehlschlagen, wenn die überwachte Software ihre Aufgaben nicht ordnungsgemäß wahrnehmen kann. Für jede dieser Kontrollen SOLLTE eine dem im Pod betriebenen Dienst angemessene Zeitspanne definieren. Auf Basis dieser Checks SOLLTE Kubernetes die Pods löschen oder neu starten.

APP.4.4.A12 Absicherung der Infrastruktur-Anwendungen (S)

Sofern eine eigene Registry für Images oder eine Software zur Automatisierung, zur Verwaltung des Festspeichers, zur Speicherung von Konfigurationsdateien oder ähnliches im Einsatz ist, SOLLTE deren Absicherung mindestens betrachten:

- Verwendung von personenbezogenen und Service-Accounts für den Zugang,
- verschlüsselte Kommunikation auf allen Netzports,
- minimale Vergabe der Berechtigungen an Benutzende und Service Accounts,
- Protokollierung der Veränderungen und
- regelmäßige Datensicherung.

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.4.4.A13 Automatisierte Auditierung der Konfiguration (H)

Es SOLLTE ein automatisches Audit der Einstellungen der Nodes, von Kubernetes und der Pods der Anwendungen gegen eine definierte Liste der erlaubten Einstellungen und gegen standardisierte Benchmarks erfolgen.

Kubernetes SOLLTE die aufgestellten Regeln im Cluster durch Anbindung geeigneter Werkzeuge durchsetzen.

APP.4.4.A14 Verwendung dedizierter Nodes (H)

In einem Kubernetes-Cluster SOLLTEN die Nodes dedizierte Aufgaben zugewiesen bekommen und jeweils nur Pods betreiben, welche der jeweiligen Aufgabe zugeordnet sind.

Bastion Nodes SOLLTEN alle ein- und ausgehenden Datenverbindungen der Anwendungen zu anderen Netzen übernehmen.

Management Nodes SOLLTEN die Pods der Control Plane betreiben und sie SOLLTEN nur die Datenverbindungen der Control Plane übernehmen.

Sofern eingesetzt, SOLLTEN Speicher-Nodes nur die Pods der Festspeicherdienste im Cluster betreiben.

APP.4.4.A15 Trennung von Anwendungen auf Node- und Cluster-Ebene (H)

Anwendungen mit einem sehr hohen Schutzbedarf SOLLTEN jeweils eigene Kubernetes-Cluster oder dedizierte Nodes nutzen, die nicht für andere Anwendungen bereitstehen.

APP.4.4.A16 Verwendung von Operatoren (H)

Die Automatisierung von Betriebsaufgaben in Operatoren SOLLTE bei besonders kritischen Anwendungen und den Programmen der Control Plane zum Einsatz kommen.

APP.4.4.A17 Attestierung von Nodes (H)

Nodes SOLLTEN eine kryptografisch und möglichst mit einem TPM verifizierte gesicherte Zustandsmeldung an die Control Plane senden. Die Control Plane SOLLTE nur Nodes in den Cluster aufnehmen, die erfolgreich ihre Unversehrtheit nachweisen konnten.

APP.4.4.A18 Verwendung von Mikro-Segmentierung (H)

Die Pods SOLLTEN auch innerhalb eines Kubernetes-Namespace nur über die notwendigen Netzports miteinander kommunizieren können. Es SOLLTEN Regeln innerhalb des CNI existieren, die alle bis auf die für den Betrieb notwendigen Netzverbindungen innerhalb des Kubernetes-Namespace unterbinden. Diese Regeln SOLLTEN Quelle und Ziel der Verbindungen genau definieren und dafür mindestens eines der folgenden Kriterien nutzen: Service-Name, Metadaten („Labels"), die Kubernetes Service Accounts oder zertifikatsbasierte Authentifizierung.

Alle Kriterien, die als Bezeichnung für diese Verbindung dienen, SOLLTEN so abgesichert sein, dass sie nur von berechtigten Personen und Verwaltungs-Diensten verändert werden können.

APP.4.4.A19 Hochverfügbarkeit von Kubernetes (H)

Der Betrieb SOLLTE so aufgebaut sein, dass bei Ausfall eines Standortes die Cluster und damit die Anwendungen in den Pods entweder ohne Unterbrechung weiterlaufen oder in kurzer Zeit an einem anderen Standort neu anlaufen können.

Für den Wiederanlauf SOLLTEN alle notwendigen Konfigurationsdateien, Images, Nutzdaten, Netzverbindungen und sonstige für den Betrieb benötigten Ressourcen inklusive der zum Betrieb nötigen Hardware bereits an diesem Standort verfügbar sein.

Für den unterbrechungsfreien Betrieb des Clusters SOLLTEN die Control Plane von Kubernetes, die Infrastruktur-Anwendungen der Cluster sowie die Pods der Anwendungen anhand von Standort-Daten der Nodes über mehrere Brandabschnitte so verteilt werden, dass der Ausfall eines Brandabschnitts nicht zum Ausfall der Anwendung führt.

APP.4.4.A20 Verschlüsselte Datenhaltung bei Pods (H)

Die Dateisysteme mit den persistenten Daten der Control Plane (hier besonders *etcd*) und der Anwendungsdienste SOLLTEN verschlüsselt werden.

APP.4.4.A21 Regelmäßiger Restart von Pods (H)

Bei einem erhöhten Risiko für Fremdeinwirkung und einem sehr hohen Schutzbedarf SOLLTEN Pods regelmäßig gestoppt und neu gestartet werden. Kein Pod SOLLTE länger als 24 Stunden laufen. Dabei SOLLTE die Verfügbarkeit der Anwendungen im Pod sichergestellt sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen im Bereich Container finden sich unter anderem in folgenden Veröffentlichungen:

- NIST 800-190
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf
- CIS Benchmark Kubernetes
  https://www.cisecurity.org/benchmark/kubernetes/
- OCI - Open Container Initiative
  https://www.opencontainers.org/
- CNCF - Cloud Native Computing Foundation
  https://www.cncf.io/

Bundesamt
für Sicherheit in der
Informationstechnik

APP.4.6 SAP ABAP-Programmierung

1. Beschreibung

1.1. Einleitung

Häufig werden in SAP-Systemen Eigenentwicklungen programmiert. Die Gründe dafür sind vielfältig, so können Geschäftsprozesse oder Anforderungen an das Reporting mit Hilfe von Eigenentwicklungen individuell an die Institution angepasst werden. Außerdem ist es möglich, spezielle Funktionen zu erstellen, die in der Standard-Auslieferung nicht vorhanden sind.

Eigenentwicklungen werden von Entwickelnden der Institution oder von beauftragten Entwickelnden programmiert. Im SAP-Umfeld wird dazu häufig ABAP (Advanced Business Application Programming) verwendet.

ABAP ist eine proprietäre, plattformunabhängige Programmiersprache des Unternehmens SAP. Sie wurde für die Programmierung kommerzieller Anwendungen im SAP-Umfeld entwickelt und ähnelt in ihrer Grundstruktur entfernt der Sprache COBOL. Wichtige Merkmale sind:

- Integration eines Authentisierungs-, Rollen- und Berechtigungskonzepts,
- Verwendung eines proprietären, datenbankunabhängigen SQL-Derivats (Open SQL),
- Unterstützung der Kommunikation zwischen verschiedenen SAP-Systemen sowie
- Integration von Audit-Optionen.

1.2. Zielsetzung

Der Baustein zeigt ABAP-Entwickelnden und Sicherheitstestenden relevante technische Risiken auf, die sich durch ABAP-Eigenentwicklungen ergeben können. Außerdem werden Anforderungen definiert, die aufzeigen, wie ABAP-Programme sicher entwickelt und eingesetzt werden können.

Der Baustein setzt grundlegende Kenntnisse in ABAP und im Umgang mit ABAP-Entwicklungswerkzeugen voraus.

1.3. Abgrenzung und Modellierung

Der Baustein APP.4.6 *SAP ABAP-Programmierung* ist auf jedes SAP-System einmal anzuwenden, wenn Eigenentwicklungen in der Programmiersprache ABAP erstellt werden.

Mit diesem Baustein werden die Bausteine CON.8 *Software-Entwicklung*, APP.6 *Allgemeine Software* und APP.7 *Entwicklung von Individualsoftware* um konkrete Aspekte zur Entwicklung von ABAP-Programmen erweitert.

Der Baustein stellt keine vollständige Anleitung dar, um ABAP-Programme zu entwickeln, sondern beschreibt die generellen Risiken der Programmiersprache ABAP. Im Baustein werden Anforderungen definiert, die bei der Entwicklung von ABAP-Programmen aus Sicherheitssicht erfüllt werden sollten.

Da Webanwendungen nur einen sehr geringen Anteil aller ABAP-Anwendungen in SAP-Implementierungen ausmachen, stehen Web-Schwachstellen nicht im Fokus dieses Dokuments.

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.4.6 *SAP ABAP-Programmierung* von besonderer Bedeutung.

2.1. Fehlende Berechtigungsprüfungen

In SAP werden Berechtigungen nur dann geprüft, wenn eine entsprechende Berechtigungsprüfung von Entwickelnden im Programm implementiert wurde. Ohne eine solche Prüfung im Programm-Code wird also nicht getestet, ob Benutzende auch wirklich berechtigt sind eine Aktion auszuführen. In selbst entwickeltem Programm-Code werden Berechtigungsprüfungen aber häufig vergessen. Somit greift das gesamte Berechtigungskonzept oftmals nicht und unberechtigte Personen können auf die im SAP-System gespeicherten Daten zugreifen. Dadurch kann etwa auch gegen Compliance-Anforderungen verstoßen werden. Dies kann besonders bei Wirtschaftsprüfungen schwerwiegende Folgen nach sich ziehen.

2.2. Verlust von Vertraulichkeit oder Integrität von kritischen Daten

SAP-Systeme enthalten viele institutionskritische Informationen. Der SAP-Standard sieht verschiedene Mechanismen vor, diese Daten zu schützen. Allerdings könnte durch fehlerhafte ABAP-Eigenentwicklungen unerlaubt auf institutionskritische Informationen zugegriffen werden. Mitarbeitende oder Angreifende könnten die Daten so in eine nicht mehr kontrollierbare Umgebung transferieren. Ebenso könnten mit Hilfe von ABAP-Programmen kritische Daten manipuliert werden, indem die Sicherheitsmechanismen des SAP-Standards umgangen werden.

2.3. Injection-Schwachstellen

Injection-Schwachstellen entstehen dadurch, dass Angreifende Steuerzeichen bzw. Kommandos über das Eingabefeld in eine Anwendung einschleust. Ein erfolgreicher Angriff kann den geplanten Programmablauf durch unerwartete Kommandos stören.

Injection-Schwachstellen stellen für Eigenentwicklungen das größte Sicherheitsrisiko dar. Durch fehlerhaften Code in einer ABAP-Anwendung können Angreifende ein SAP-System mitunter vollständig kontrollieren. Da solche Angriffe sehr komplex sind und es viele Varianten davon gibt, lassen sie sich ohne spezielle Schulungen kaum erkennen und beheben.

2.4. Umgehung von vorhandenen SAP-Sicherheitsmechanismen

Der SAP-Standard stellt verschiedene Schutzmechanismen für Daten zur Verfügung. Dazu gehören unter anderem die Mandantentrennung, Identity-Management sowie Rollen und Berechtigungen. Diese Sicherheitsmechanismen können im Code jedoch bewusst umgangen oder ungewollt weggelassen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.6 *SAP ABAP-Programmierung* 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	Entwickelnde
Weitere Zuständigkeiten	Keine

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.4.6.A1 Absicherung von Reports mit Berechtigungsprüfungen (B)

Es MUSS sichergestellt sein, dass nur berechtigte Personen selbst programmierte Auswertungen (Reports) starten können. Deswegen MUSS jeder Report explizite, zum Kontext passende Berechtigungsprüfungen durchführen.

APP.4.6.A2 Formal korrekte Auswertung von Berechtigungsprüfungen (B)

Jede Berechtigungsprüfung im Code MUSS durch Abfrage des Rückgabewertes *SY-SUBRC* ausgewertet werden.

APP.4.6.A3 Berechtigungsprüfung vor dem Start einer Transaktion (B)

Wenn Entwickelnde den Befehl *CALL TRANSACTION* verwenden, MUSS vorher immer eine Startberechtigungsprüfung durchgeführt werden.

APP.4.6.A4 Verzicht auf proprietäre Berechtigungsprüfungen (B)

Jede Berechtigungsprüfung MUSS technisch über den dafür vorgesehenen Befehl *AUTHORITY-CHECK* erfolgen. Proprietäre Berechtigungsprüfungen, z. B. basierend auf Konto-Kennungen, DÜRFEN NICHT benutzt 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.4.6.A5 Erstellung einer Richtlinie für die ABAP-Entwicklung (S)

Es SOLLTE eine Richtlinie für die Entwicklung von ABAP-Programmen erstellt werden. Die Richtlinie SOLLTE neben Namenskonventionen auch Vorgaben zu ABAP-Elementen beinhalten, die verwendet bzw. nicht verwendet werden dürfen. Die Anforderungen aus diesem Baustein SOLLTEN in die Richtlinie aufgenommen werden. Die Richtlinie SOLLTE für die Entwickelnden verbindlich sein.

APP.4.6.A6 Vollständige Ausführung von Berechtigungsprüfungen (S)

Bei einer Berechtigungsprüfung im ABAP-Code (*AUTHORITY-CHECK <OBJECT>*) SOLLTE sichergestellt sein, dass alle Felder des relevanten Berechtigungsobjekts überprüft werden. Wenn einzelne Felder tatsächlich nicht benötigt werden, SOLLTEN sie als *DUMMY* gekennzeichnet werden. Zusätzlich SOLLTE am Feld der Grund für die Ausnahme dokumentiert werden.

APP.4.6.A7 Berechtigungsprüfung während der Eingabeverarbeitung (S)

Funktionscodes und Bildschirmelemente von ABAP-Dynpro-Anwendungen SOLLTEN konsistent sein. Wenn ein Bildschirmelement abgeschaltet wurde, dann SOLLTE eine Anwendung NICHT ohne adäquate Berechtigungsprüfungen auf Ereignisse dieses Elements reagieren. Wenn bestimmte Einträge eines Dynpro-Menüs ausgeblendet oder einzelne Schaltflächen deaktiviert werden, dann SOLLTEN auch die zugehörigen Funktionscodes nicht ausgeführt werden.

APP.4.6.A8 Schutz vor unberechtigten oder manipulierenden Zugriffen auf das Dateisystem (S)

Wenn Zugriffe auf Dateien des SAP-Servers von Eingaben der Benutzenden abhängen, SOLLTEN diese Eingaben vor dem Zugriff validiert werden.

APP.4.6.A9 Berechtigungsprüfung in remote-fähigen Funktionsbausteinen (S)

Es SOLLTE sichergestellt werden, dass alle remote-fähigen Funktionsbausteine im Programmcode explizit prüfen, ob der Aufrufende berechtigt ist, die zugehörige Businesslogik auszuführen.

APP.4.6.A10 Verhinderung der Ausführung von Betriebssystemkommandos (S)

Jedem Aufruf eines erlaubten Betriebssystemkommandos SOLLTE eine entsprechende Berechtigungsprüfung (Berechtigungsobjekt *S_LOG_COM*) vorangestellt werden. Eingaben von Benutzenden SOLLTEN NICHT Teil eines Kommandos sein. Deswegen SOLLTEN Betriebssystemaufrufe ausschließlich über dafür vorgesehene SAP-Standardfunktionsbausteine ausgeführt werden.

APP.4.6.A11 Vermeidung von eingeschleustem Schadcode (S)

Die ABAP-Befehle *INSERT REPORT* und *GENERATE SUBROUTINE POOL* SOLLTEN NICHT verwendet werden.

APP.4.6.A12 Vermeidung von generischer Modulausführung (S)

Transaktionen, Programme, Funktionsbausteine und Methoden SOLLTEN NICHT generisch ausführbar sein. Sollte es wichtige Gründe für eine generische Ausführung geben, SOLLTE detailliert dokumentiert werden, wo und warum dies geschieht. Zusätzlich SOLLTE eine Allowlist definiert werden, die alle erlaubten Module enthält. Bevor ein Modul aufgerufen wird, SOLLTE die Eingabe von Benutzenden mit der Allowlist abgeglichen werden.

APP.4.6.A13 Vermeidung von generischem Zugriff auf Tabelleninhalte (S)

Tabelleninhalte SOLLTEN NICHT generisch ausgelesen werden. Sollte es wichtige Gründe dafür geben, dies doch zu tun, SOLLTE detailliert dokumentiert werden, wo und warum dies geschieht. Außerdem SOLLTE dann gewährleistet sein, dass sich der dynamische Tabellenname auf eine kontrollierbare Liste von Werten beschränkt.

APP.4.6.A14 Vermeidung von nativen SQL-Anweisungen (S)

Die Schnittstelle ABAP Database Connectivity (ADBC) SOLLTE NICHT verwendet werden. Eingaben von Benutzenden SOLLTEN NICHT Teil von ADBC-Befehlen sein.

APP.4.6.A15 Vermeidung von Datenlecks (S)

Es SOLLTE eine ausreichend sichere Berechtigungsprüfung durchgeführt werden, bevor geschäftskritische Daten angezeigt, übermittelt oder exportiert werden. Vorgesehene (gewollte) Möglichkeiten des Exports SOLLTEN dokumentiert werden.

APP.4.6.A16 Verzicht auf systemabhängige Funktionsausführung (S)

ABAP-Programme SOLLTEN NICHT systemabhängig programmiert werden, so dass sie nur auf einem bestimmten SAP-System ausgeführt werden können. Sollte dies jedoch unbedingt erforderlich sein, SOLLTE es detailliert dokumentiert werden. Außerdem SOLLTE der Code dann manuell überprüft werden.

APP.4.6.A17 Verzicht auf mandantenabhängige Funktionsausführung (S)

ABAP-Programme SOLLTEN NICHT mandantenabhängig programmiert werden, so dass sie nur von einem bestimmten Mandanten ausgeführt werden können. Sollte dies jedoch unbedingt erforderlich sein, SOLLTE es detailliert dokumentiert werden. Außerdem SOLLTEN dann zusätzliche Sicherheitsmaßnahmen ergriffen werden, wie beispielsweise eine manuelle Code-Überprüfung (manuelles Code-Review) oder eine Qualitätssicherung auf dem entsprechenden Mandanten.

APP.4.6.A18 Vermeidung von Open-SQL-Injection-Schwachstellen (S)

Dynamisches Open SQL SOLLTE NICHT verwendet werden. Falls Datenbankzugriffe mit dynamischen SQL-Bedingungen notwendig sind, SOLLTEN KEINE Eingaben von Benutzenden in der jeweiligen Abfrage übertragen werden. Wenn das dennoch der Fall ist, SOLLTEN die Eingaben von Benutzenden zwingend geprüft werden (Output Encoding).

APP.4.6.A19 Schutz vor Cross-Site-Scripting (S)

Auf selbst entwickeltes HTML in Business-Server-Pages-(*BSP*)-Anwendungen oder HTTP-Handlern SOLLTE möglichst verzichtet werden.

APP.4.6.A20 Keine Zugriffe auf Daten eines anderen Mandanten (S)

Die automatische Mandantentrennung SOLLTE NICHT umgangen werden. Auf Daten anderer Mandanten SOLLTE NICHT mittels *EXEC SQL* oder der Open SQL Option *CLIENT SPECIFIED* zugegriffen werden.

APP.4.6.A21 Verbot von verstecktem ABAP-Quelltext (S)

Der Quelltext eines selbst erstellten ABAP-Programms SOLLTE immer lesbar sein. Techniken, die das verhindern (Obfuskation), SOLLTEN NICHT verwendet werden.

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.4.6.A22 Einsatz von ABAP-Codeanalyse Werkzeugen (H)

Zur automatisierten Überprüfung von ABAP-Code auf sicherheitsrelevante Programmierfehler, funktionale und technische Fehler sowie auf qualitative Schwachstellen SOLLTE ein ABAP-Codeanalyse-Werkzeug eingesetzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Im „Best Practice Guide: Leitfaden Development ABAP 2.0“ der Deutschsprachigen SAP Anwendergruppe e.V. (DSAG) finden sich vertiefende Informationen zur ABAP-Programmierung.

Weitere Informationen und Best Practices zur sicheren ABAP-Programmierung finden sich im Buch „Sichere ABAP-Programmierung“ von Wiegenstein, Schuhmacher, Schinzel, Weidemann aus dem SAP Press Verlag.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.5.2 Microsoft Exchange und Outlook

1. Beschreibung

1.1. Einleitung

Microsoft Exchange Server (im Folgenden „Exchange“) ist eine Groupware-Lösung für mittlere bis große Institutionen. Mit ihr können elektronisch Nachrichten übermittelt werden und sie verfügt über weitere Dienste, um Workflows zu unterstützen. Nachrichten, wie E-Mails, können mit Exchange zentral verwaltet, zugestellt, gefiltert und versendet werden. Ebenso können typische Groupware-Anwendungen, wie Notizen, Kontaktlisten, Kalender und Aufgabenlisten angeboten und verwaltet werden. Um die Funktionen von Exchange nutzen zu können, ist neben dem Server-Dienst eine zusätzliche Client-Software oder ein Webbrowser nötig.

Microsoft Outlook (im Folgenden „Outlook“) ist ein Client für Exchange, der durch die Installation des Office-Pakets von Microsoft oder durch Integration in die Betriebssysteme von mobilen Geräten direkt zur Verfügung gestellt wird. Darüber hinaus ermöglicht die Webanwendung „Outlook im Web“ (ehemals „Outlook Web App“) über den Browser z. B. auf E-Mails, Kontakte und den Kalender zuzugreifen. Diese Funktion ist in Exchange bereits enthalten.

Die Kombination aus Exchange-Servern und Outlook-Clients wird in diesem Baustein als Exchange-System bezeichnet.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es, über typische Gefährdungen für Exchange und Outlook zu informieren sowie aufzuzeigen, wie Exchange und Outlook sicher in Institutionen eingesetzt werden.

1.3. Abgrenzung und Modellierung

Der Bausteine ist auf alle Exchange-Systeme im Informationsverbund anzuwenden.

Allgemeine Anforderungen an die Sicherheit von E-Mail-Systemen sind im Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* zu finden. Er ist zusätzlich auf jedes E-Mail-System anzuwenden, das auf Exchange bzw. Outlook basiert.

Der Baustein enthält spezifische Gefährdungen und Anforderungen für Exchange-Systeme. Spezifische Anforderungen an Serverplattformen und Betriebssysteme sind nicht Bestandteil des Bausteins. Diese

sind in den Bausteinen SYS.1.1 *Allgemeiner Server* sowie SYS.2.1 *Allgemeiner Client* und in den jeweiligen betriebssystemspezifischen Bausteinen zu finden.

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.5.2 *Microsoft Exchange und Outlook* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für Exchange und Outlook

Übergreifende Regelungen und Vorgaben für Exchange und Outlook sind notwendig, damit die Sicherheit der Informationen, die mit Exchange und Outlook verarbeitet werden, gewährleistet wird. Beispielsweise können Daten verloren gehen, ungewollt verändert oder gelöscht werden, wenn Exchange fehlerhaft und ungeregelt in das Active Directory eingebunden wird. Ähnliches gilt, wenn Postfachdatenbanken ungeregelt depubliziert werden und Exchange unzureichend in der Sicherheitsrichtlinie berücksichtigt wird. Gleiches gilt, wenn die Outlook-Clients ungeregelt auf die Exchange-Server zugreifen können.

2.2. Fehlerhafte Migration von Exchange

Exchange-Systeme werden in der Praxis häufiger migriert als neu installiert. Um auf eine neue Version des Exchange Servers zu migrieren, muss in einigen Fällen das Betriebssystem auf eine neuere Version aktualisiert werden. Neue Versionen der Betriebssysteme stellen ihrerseits oft Anforderungen an das bestehende Domänenkonzept und die existierenden Verzeichnisdienste.

Wenn die Migration nicht sorgfältig geplant und durchgeführt wird, kann die interne Kommunikation über Exchange in der Institution massiv gestört werden, was in der Folge die Produktivität verringern könnte. Während der Migration können Probleme bei der Konfiguration auftreten, indem sich z. B. die Konfigurationseinstellungen für die unterschiedlichen Versionen oder die Möglichkeiten zur Anbindung an Verzeichnisdienste geändert haben. Des Weiteren können fehlerhafte Protokolleinstellungen zu Unregelmäßigkeiten bei der Informationsübermittlung, Authentisierung und Verschlüsselung führen.

2.3. Unzulässiger Browserzugriff auf Exchange

Mit Exchange können Anwendende über einem Browser auf das eigene E-Mail-Konto zugreifen. Hierzu werden die Internet Information Services (IIS) verwendet, die Bestandteil des Windows-Betriebssystems sind. Wenn diese Funktion unsachgemäß geplant und fehlerhaft konfiguriert wird, kann unter Umständen unkontrolliert von außen auf das interne Netz zugegriffen werden.

Wenn über das Internet mit einem Browser auf die E-Mails zugegriffen werden soll, birgt dies ein großes Gefahrenpotenzial. Ohne direkten Zugriff auf das Netz der Institution könnten Angreifende auf die E-Mails zugreifen und so unter anderem E-Mail-Adressen und -Inhalte ausspähen, E-Mail-Funktionen missbrauchen, Spam-Mails verschicken sowie Zugang zu institutionsinternen Informationen erhalten.

2.4. Unerlaubte Anbindung anderer Systeme an Exchange

Exchange-Systeme sind eng mit dem Betriebssystem Windows verzahnt und arbeiten durch sogenannte Konnektoren (auch Connectors genannt) mit Fremdsystemen zusammen. Mithilfe der

Konnektoren ist es anderen E-Mail-Systemen möglich, über bestimmte Protokolle (z. B. POP3) E-Mails von Exchange-Servern abzurufen.

Wenn bei der Installation oder einer Migration von Exchange die Konnektoren nicht mit berücksichtigt werden, können die vorhandenen Konnektoren inkompatibel zu der migrierten Exchange-Version sein. Hierdurch können E-Mails verloren gehen oder ungewollt verändert werden.

Außerhalb des homogenen Microsoft-Umfelds sind Sicherheitseinstellungen, die sich auf das Exchange-System beziehen, ungültig.

Wenn verschiedene Teilsysteme separat administriert werden, können stets Inkonsistenzen auftreten. Unsachgemäß angebundene Fremdsysteme können zudem zur Folge haben, dass Daten verloren gehen oder das Exchange-System blockiert wird.

2.5. Fehlerhafte Administration von Zugangs- und Zugriffsrechten unter Exchange und Outlook

Werden Zugangsrechte zu einem Outlook-Client bzw. auf innerhalb von Exchange und Outlook gespeicherte Daten fehlerhaft angelegt und administriert, können Sicherheitslücken entstehen. Dies ist beispielsweise der Fall, wenn über die notwendigen Rechte hinaus zusätzliche Rechte vergeben werden und dadurch unberechtigte Personen auf vertrauliche Informationen zugreifen können.

2.6. Fehlerhafte Konfiguration von Exchange

Eine häufige Ursache für erfolgreiche Angriffe auf Dienste wie Exchange sind fehlerhaft konfigurierte Exchange-Systeme. Da ein Exchange-System sehr komplex ist, können durch diverse Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter zahlreiche Sicherheitsprobleme entstehen. Die möglichen Fehlkonfigurationen erstrecken sich von der Installation und dem Betrieb der Exchange-Komponenten auf ungeeigneten IT-Systemen über nicht getätigte Verschlüsselungen und unzureichende Zugriffsbeschränkungen auf Exchange-Servern bis hin zur fehlerhaften Rechtevergabe bei der Erzeugung oder Initialisierung einer Exchange-Datenbank.

2.7. Fehlerhafte Konfiguration von Outlook

Der E-Mail-Client Outlook ist ein wichtiger Teil des Exchange-Systems. Für die Gesamtsicherheit des Exchange-Systems ist es wichtig, dass die Clients korrekt konfiguriert sind. Schon das ausgewählte Kommunikationsprotokoll kann spezielle Sicherheitsprobleme nach sich ziehen. Ebenso könnten private Schlüssel kompromittiert werden, mit denen E-Mails verschlüsselt und signiert werden. Wird auf Netzebene verschlüsselt, z. B. durch IPSec oder TLS, kann dieser Verschlüsselungsmechanismus bei einem fehlerhaft konfigurierten Client unwirksam werden. Durch Fehlkonfiguration können Sicherheitsprobleme entstehen, z. B. der Verlust der Vertraulichkeit durch unbefugten Zugriff.

2.8. Fehlfunktionen und Missbrauch selbst entwickelter Makros sowie Programmierschnittstellen unter Outlook

Viele Softwareherstellende sehen in ihren Tools und Anwendungen Programmierschnittstellen vor, sogenannte Application Programming Interfaces (APIs). Diese erlauben es, bestimmte Funktionen auch aus anderen Programmen heraus zu nutzen oder den Funktionsumfang der Anwendung zu erweitern. Solche Funktionen in Outlook können missbraucht werden, um Schadsoftware zu verbreiten. Zu den Schadsoftwarevarianten zählen z. B. bösartige Tools und Makros, die direkt Outlook und die damit verbundenen E-Mail-Funktionen ausnutzen, um Informationen abzugreifen, zu verändern oder zu löschen. Makros wiederum können dazu genutzt werden, Nachrichten, Termine oder Aufgaben weiterzuleiten oder zu verschieben. Dabei können Fehler in Makros ein erhöhtes Risiko darstellen. Indexfehler innerhalb von Makros können zu falschen Ergebnissen und zu möglicherweise

unwirtschaftlichen Entscheidungen in der Institution führen. Spezifische Folgen können unnötige Kosten oder ein automatisierter Datenabfluss sein.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.5.2 *Microsoft Exchange und Outlook* 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	Keine

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.5.2.A1 Planung des Einsatzes von Exchange und Outlook (B)

Bevor Exchange und Outlook eingesetzt werden, MUSS die Institution deren Einsatz sorgfältig planen. Dabei MUSS sie mindestens folgende Punkte beachten:

- Aufbau der E-Mail-Infrastruktur,
- einzubindende Clients beziehungsweise Server,
- Nutzung von funktionalen Erweiterungen sowie
- die zu verwendenden Protokolle.

APP.5.2.A2 Auswahl einer geeigneten Exchange-Infrastruktur (B)

Der IT-Betrieb MUSS auf Basis der Planung des Einsatzes von Exchange entscheiden, mit welchen IT-Systemen und Anwendungskomponenten sowie in welcher hierarchischen Abstufung die Exchange-Infrastruktur realisiert wird. Im Rahmen der Auswahl MUSS auch entschieden werden, ob die Exchange-Systeme als Cloud- oder lokaler Dienst betrieben werden sollen.

APP.5.2.A3 Berechtigungsmanagement und Zugriffsrechte (B)

Zusätzlich zum allgemeinen Berechtigungskonzept MUSS die Institution ein Berichtigungskonzept für die Systeme der Exchange-Infrastruktur erstellen, geeignet dokumentieren und anwenden.

Der IT-Betrieb MUSS serverseitige Benutzendenprofile für einen rechnerunabhängigen Zugriff der Benutzenden auf Exchange-Daten verwenden. Er MUSS die Standard-NTFS-Berechtigungen für das Exchange-Verzeichnis so anpassen, dass nur autorisierte Administrierende und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.

APP.5.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.5.2.A5 Datensicherung von Exchange (B)

Exchange-Server MÜSSEN vor Installationen und Konfigurationsänderungen sowie in zyklischen Abständen gesichert werden. Dabei MÜSSEN insbesondere die Exchange-Server-Datenbanken gesichert werden.

Gelöschte Exchange-Objekte SOLLTEN erst nach einiger Zeit aus der Datenbank entfernt 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.5.2.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.5.2.A7 Migration von Exchange-Systemen (S)

Der IT-Betrieb SOLLTE alle Migrationsschritte gründlich planen und dokumentieren. Der IT-Betrieb SOLLTE dabei Postfächer, Objekte, Sicherheitsrichtlinien, Active-Directory-Konzepte sowie die Anbindung an andere E-Mail-Systeme berücksichtigen. Außerdem SOLLTE er Funktionsunterschiede zwischen verschiedenen Versionen von Exchange beachten. Das neue Exchange-System SOLLTE, bevor es installiert wird, in einem separaten Testnetz geprüft werden.

APP.5.2.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.5.2.A9 Sichere Konfiguration von Exchange-Servern (S)

Der IT-Betrieb SOLLTE Exchange-Server entsprechend der Vorgaben aus der Sicherheitsrichtlinie installieren und konfigurieren. Konnektoren SOLLTEN sicher konfiguriert werden. Der IT-Betrieb SOLLTE die Protokollierung des Exchange-Systems aktivieren. Für vorhandene benutzendenspezifische Anpassungen SOLLTE ein entsprechendes Konzept erstellt werden.

Bei der Verwendung von funktionalen Erweiterungen SOLLTE sichergestellt sein, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit weiterhin erfüllt sind.

APP.5.2.A10 Sichere Konfiguration von Outlook (S)

Der IT-Betrieb SOLLTE für jeden Benutzenden ein eigenes Outlook-Profil mit benutzendenspezifischen Einstellungen anlegen.

Der IT-Betrieb SOLLTE Outlook so konfigurieren, dass nur notwendige Informationen an andere Benutzende übermittelt werden. Der IT-Betrieb SOLLTE die Benutzenden darüber informieren, welche Informationen automatisiert an andere Benutzende übermittelt werden. Lesebestätigungen und Informationen, die auf die interne Struktur der Institution schließen lassen, SOLLTEN NICHT an Externe übermittelt werden.

APP.5.2.A11 Absicherung der Kommunikation zwischen Exchange-Systemen (S)

Der IT-Betrieb SOLLTE nachvollziehbar entscheiden, mit welchen Schutzmechanismen die Kommunikation zwischen Exchange-Systemen abgesichert wird. Insbesondere SOLLTE der IT-Betrieb festlegen, wie die Kommunikation zu folgenden Schnittstellen abgesichert wird:

- Administrationsschnittstellen,
- Client-Server-Kommunikation,
- vorhandene Web-based-Distributed-Authoring-and-Versioning-(WebDAV)-Schnittstellen,

- Server-Server-Kommunikation und
- Public-Key-Infrastruktur, auf der die E-Mail-Verschlüsselung von Outlook basiert.

APP.5.2.A12 Einsatz von Outlook Anywhere, MAPI over HTTP und Outlook im Web (S)

Der IT-Betrieb SOLLTE Outlook Anywhere, MAPI over HTTP und Outlook im Web entsprechend den Sicherheitsanforderungen der Institution konfigurieren. Der Zugriff auf Exchange über das Internet SOLLTE auf die notwendigen Benutzenden beschränkt werden.

APP.5.2.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.5.2.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.5.2.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.5.2.A16 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.5.2.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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.5.2.A17 Verschlüsselung von Exchange-Datenbankdateien (H)

Der IT-Betrieb SOLLTE ein Konzept für die Verschlüsselung von PST-Dateien und Informationsspeicher-Dateien erstellen. Die Institution SOLLTE die Benutzenden über die Funktionsweise und die Schutzmechanismen bei der Verschlüsselung von PST-Dateien informieren. Weitere Aspekte für lokale PST-Dateien, die berücksichtigt werden SOLLTEN, wenn Exchange-Systemdatenbanken verschlüsselt werden, sind:

- eigene Verschlüsselungsfunktionen,
- Verschlüsselungsgrade sowie
- Mechanismen zur Absicherung der Daten in einer PST-Datei.

Mechanismen wie z. B. Encrypting File System oder Windows BitLocker Laufwerkverschlüsselung SOLLTEN zur Absicherung der PST-Dateien genutzt werden.

APP.5.2.A18 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Microsoft stellt auf seiner Webseite „Microsoft Technet" (https://technet.microsoft.com/de-de) umfangreiche Informationen zur Administration von Microsoft Exchange zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.5.3 Allgemeiner E-Mail-Client und -Server

1. Beschreibung

1.1. Einleitung

E-Mail ist eine der am häufigsten genutzten und ältesten Internetanwendungen. E-Mails werden dazu verwendet, Texte und angehängte Dateien zu versenden. Dazu wird eine E-Mail-Adresse benötigt.

Um E-Mail nutzen zu können, werden E-Mail-Server benötigt, die elektronische Nachrichten empfangen und versenden. In der Regel rufen E-Mail-Clients, mit denen auf E-Mail-Dienste zugegriffen wird, Nachrichten, die für sie bestimmt sind, mittels der Protokolle POP3 oder IMAP vom E-Mail-Server ab und senden mit dem Protokoll SMTP selbst Nachrichten an den E-Mail-Server, der diese bei Bedarf an einen anderen E-Mail-Server weiterleitet.

Da E-Mail insbesondere in Unternehmen und Behörden weit verbreitet ist, sind E-Mail-Server häufig das Ziel von Angriffen.

Auch E-Mail-Clients stehen im Fokus von Angriffen. Sie werden angegriffen, indem beispielsweise Schadsoftware per E-Mail versendet wird. Zusätzlich werden E-Mails auch oft als Werkzeug für Social-Engineering-Angriffe eingesetzt.

Aus diesen Gründen kommt dem sicheren Betrieb und der sicheren Nutzung von E-Mail-Anwendungen eine besondere Bedeutung zu.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationen zu schützen, die mit E-Mail-Clients bzw. auf E-Mail-Servern verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* ist auf jeden E-Mail-Client und -Server im Informationsverbund anzuwenden.

Der Baustein enthält Anforderungen für allgemeine E-Mail-Clients und -Server. Anforderungen für Serverplattformen, Betriebssysteme und Clients sind nicht Bestandteil des Bausteins. Diese sind in den

Bausteinen SYS.1.1 *Allgemeiner Server* sowie SYS.2.1 *Allgemeiner Client* und in den jeweiligen betriebssystemspezifischen Bausteinen zu finden.

Der Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* wird in einem Informationsverbund meist in Verbindung mit einem weiteren spezifischen Baustein der Schicht APP.5 *E-Mail/Groupware/Kommunikation* genutzt. Diese müssen ebenfalls separat umgesetzt werden. Zu diesen Bausteinen zählt unter anderem APP.5.2 *Microsoft Exchange und Outlook*.

Anforderungen für die Protokollierung und Datensicherung finden sich in den Bausteinen OPS.1.1.5 *Protokollierung* und CON.3 *Datensicherungskonzept*.

Nicht in diesem Baustein behandelt werden Groupware-Funktionen, die neben E-Mail auch noch weitere Funktionen wie die Verwaltung von Kontaktdaten und Kalendern bieten. Ebenso werden keine reinen Cloud-Lösungen behandelt, wie sie etwa als Teil von Microsoft 365 oder Google G Suite zu finden sind. Allgemeine Anforderungen dazu sind im Baustein OPS.2.2 *Cloud-Nutzung* zu finden. Ebenfalls nicht betrachtet werden Webbrowser, mit denen über Webseiten auf Webmail-Dienste zugegriffen wird. Anforderungen an Webbrowser sind im Baustein APP.1.2 *Webbrowser* zu finden.

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.5.3 *Allgemeiner E-Mail-Client und -Server* von besonderer Bedeutung.

2.1. Unzureichende Planung der E-Mail-Nutzung

E-Mail-Anwendungen können ohne entsprechend dokumentierte Regelungen und ein definiertes Sicherheitsverfahren in der Institution nicht sicher genutzt werden. Falls in der Planung der E-Mail-Systeme die prozessualen, organisatorischen und technischen Regelungen vernachlässigt werden, könnte dies interne sowie externe Angriffe zur Folge haben.

Beispielsweise kann ein zu klein dimensionierter E-Mail-Server durch eine große Zahl von eingehenden E-Mails ausfallen. Werden keine ausreichenden Sicherheitsmaßnahmen geplant, ist es auch möglich, dass die E-Mail-Clients anfälliger für E-Mails sind, die Schadsoftware enthalten.

2.2. Fehlerhafte Einstellung von E-Mail-Clients und -Servern

Da eine E-Mail-Infrastruktur sehr komplex sein kann, können durch die vielen möglichen Einstellungen und durch die sich gegenseitig beeinflussenden Parameter zahlreiche Sicherheitsprobleme entstehen.

Beispielsweise kann ein E-Mail-Server durch eine fehlerhafte Konfiguration legitime E-Mails von anderen Servern ablehnen. Zusätzlich wäre es möglich, dass essenzielle Einstellungen ignoriert oder missachtet werden, z. B. die Transportverschlüsselung von E-Mails.

Außerdem kann eine falsche Konfiguration in E-Mail-Clients dazu führen, dass diese Schadcode in E-Mails ausführen. Diese Sicherheitslücken können zu einem signifikanten Verlust der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen führen.

Viele Institutionen setzen keine Sicherheitsmechanismen ein, die es anderen E-Mail-Servern ermöglichen, zu überprüfen, ob eine E-Mail tatsächlich von der angegebenen Absendeadresse stammt. Außerdem kann ein falsch eingestellter E-Mail-Server dazu missbraucht werden, um Spam-E-Mails zu versenden.

2.3. Unzuverlässigkeit von E-Mail

Über E-Mail-Anwendungen lassen sich schnell und komfortabel Daten austauschen. Das ist jedoch nicht immer zuverlässig. Zum Beispiel können durch fehlerhafte E-Mail-Server oder gestörte Übertragungswege Nachrichten verloren gehen. Ursachen dafür sind beispielsweise Spam-Filter, die legitime Nachrichten herausfiltern und verwerfen. E-Mails können auch verloren gehen, wenn die Zieladresse nicht korrekt angegeben wurde. Im schlimmsten Fall können vertrauliche Informationen an falsche Zieladressen gesendet worden sein.

2.4. Schadsoftware in E-Mails

Es gibt verschiedene Wege, wie bei einem Angriff Schadsoftware mit Hilfe von E-Mails verbreitet werden kann. Einerseits kann schädlicher Code direkt in einer E-Mail enthalten sein. Ist der E-Mail-Client nicht richtig konfiguriert, wird der Code beim Öffnen der E-Mail ausgeführt.

Eine weitere Möglichkeit besteht darin, dass Dateien mit Schadsoftware als Anhang von E-Mails versendet werden. Falls solche E-Mails nicht durch Spam- oder Virenfilter aussortiert werden und die Anhänge geöffnet werden, wird die Schadsoftware ausgeführt. Diese kann zu weitreichenden Schäden auch für andere IT-Systeme führen, wenn beispielsweise Ransomware (oft als „Erpressungstrojaner“ bezeichnet) ausgeführt wird.

2.5. Social Engineering

E-Mails werden oft bei Angriffen dazu eingesetzt, um vertrauliche Informationen zu erhalten oder Personal zu anderem schädlichen Verhalten zu verleiten. Beispielsweise kann bei einem Angriff eine E-Mail gesendet werden, die vermeintlich von Vorgesetzten stammt und Anweisungen enthält, die der Institution schaden (sogenannter CEO-Fraud). Häufig wird dabei angewiesen, dass Geld auf Konten im Ausland überwiesen werden soll.

Möglich ist auch, dass eine gefälschte E-Mail einer eigentlich vertrauenswürdigen Quelle dazu auffordert, Zugangsdaten auf einer Webseite einzugeben (Phishing). Die so gewonnenen Zugangsdaten können dann bei einem Angriff für weitere Aktionen verwendet werden.

Verstärkt wird die Gefahr von Social Engineering, wenn die Institution nicht regelmäßig zu diesen Gefährdungen schult und sensibilisiert.

2.6. Mitlesen und Manipulieren von E-Mails

E-Mails werden in der Regel unverschlüsselt und ohne digitale Signatur versendet. Deswegen können bei einem Angriff E-Mails mitgelesen und sogar beliebig verändert werden. Auf diesem Weg können vertrauliche Informationen offengelegt oder falsche Informationen verteilt werden. Es ist auch möglich, dass auf diesem Weg Schadsoftware eingespielt wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bau*steins* APP.5.3 *Allgemeiner E-Mail-Client und -Server* 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	Benutzende, Vorgesetzte

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.5.3.A1 Sichere Konfiguration der E-Mail-Clients (B)

Die Institution MUSS eine sichere Konfiguration für die E-Mail-Clients vorgeben. Die E-Mail-Clients MÜSSEN den Benutzenden vorkonfiguriert zur Verfügung gestellt werden.

Die Institution SOLLTE sicherstellen, dass sicherheitsrelevante Teile der Konfiguration nicht von Benutzenden geändert werden können. Ist dies nicht möglich, MUSS die Institution darauf hinweisen, dass die Konfiguration nicht selbstständig geändert werden darf.

Bevor Dateianhänge aus E-Mails geöffnet werden, MÜSSEN sie auf Schadsoftware überprüft werden. Die Dateianhänge MÜSSEN auf dem Client oder auf dem E-Mail-Server überprüft werden. E-Mail-Clients MÜSSEN so konfiguriert werden, dass sie eventuell vorhandenen HTML-Code und andere aktive Inhalte in E-Mails nicht automatisch interpretieren. Vorschaufunktionen für Datei-Anhänge MÜSSEN so konfiguriert werden, dass sie Dateien nicht automatisch interpretieren. E-Mail-Filterregeln sowie die automatische Weiterleitung von E-Mails MÜSSEN auf notwendige Anwendungsfälle beschränkt werden.

E-Mail-Clients MÜSSEN für die Kommunikation mit E-Mail-Servern über nicht vertrauenswürdige Netze eine sichere Transportverschlüsselung einsetzen.

APP.5.3.A2 Sicherer Betrieb von E-Mail-Servern (B)

Für den E-Mail-Empfang über nicht vertrauenswürdige Netze MÜSSEN E-Mail-Server eine sichere Transportverschlüsselung anbieten. Der Empfang von E-Mails über unverschlüsselte Verbindungen SOLLTE deaktiviert werden. Versenden E-Mail-Server von sich aus E-Mails an andere E-Mail-Server, SOLLTEN sie eine sichere Transportverschlüsselung nutzen. Der IT-Betrieb SOLLTE den E-Mail-Versand durch unsichere Netze über unverschlüsselte Verbindungen deaktivieren.

Der IT-Betrieb MUSS den E-Mail-Server so konfigurieren, dass E-Mail-Clients nur über eine sichere Transportverschlüsselung auf Postfächer zugreifen können, wenn dies über nicht vertrauenswürdige Netze passiert.

Die Institution MUSS alle erlaubten E-Mail-Protokolle und Dienste festlegen. Der IT-Betrieb MUSS Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergreifen. Werden Nachrichten auf einem E-Mail-Server gespeichert, MUSS der IT-Betrieb eine geeignete Größenbeschränkung für das serverseitige Postfach einrichten und dokumentieren. Außerdem MUSS der IT-Betrieb den E-Mail-Server so einstellen, dass er nicht als Spam-Relay missbraucht werden kann.

APP.5.3.A3 Datensicherung und Archivierung von E-Mails (B)

Der IT-Betrieb MUSS die Daten der E-Mail-Server und -Clients regelmäßig sichern. Dafür MUSS die Institution regeln, wie die gesendeten und empfangenen E-Mails der E-Mail-Clients sowie die E-Mails auf den Servern gesichert werden. Die Institution SOLLTE ebenfalls bei der Archivierung beachten, dass E-Mails möglicherweise nur lokal auf Clients gespeichert sind.

APP.5.3.A4 Spam- und Virenschutz auf dem E-Mail-Server (B)

Der IT-Betrieb MUSS sicherstellen, dass auf E-Mail-Servern eingehende und ausgehende E-Mails, insbesondere deren Anhänge, auf Spam-Merkmale und schädliche Inhalte überprüft werden. Die

Einführung und Nutzung von E-Mail-Filterprogrammen MUSS mit den Datenschutzbeauftragten und der Personalvertretung abgestimmt werden.

Die Institution MUSS festlegen, wie mit verschlüsselten E-Mails zu verfahren ist, wenn diese nicht durch das Virenschutzprogramm entschlüsselt werden können.

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.5.3.A5 Festlegung von Vertretungsregelungen bei E-Mail-Nutzung (S) [Vorgesetzte]

Die Institution SOLLTE Vertretungsregelungen für die Bearbeitung von E-Mails festlegen. Werden E-Mails weitergeleitet, SOLLTEN die Vertretenen mindestens darüber informiert werden. Bei der Weiterleitung von E-Mails MÜSSEN datenschutzrechtliche Aspekte berücksichtigt werden. Die Institution SOLLTE für Autoreply-Funktionen in E-Mail-Programmen Regelungen etablieren, die beschreiben, wie diese Funktionen sicher verwendet werden können. Wenn die Autoreply-Funktion benutzt wird, SOLLTEN keine internen Informationen weitergegeben werden.

APP.5.3.A6 Festlegung einer Sicherheitsrichtlinie für E-Mail (S)

Die Institution SOLLTE eine Sicherheitsrichtlinie für die Nutzung von E-Mails erstellen und regelmäßig aktualisieren. Die Institution SOLLTE alle Benutzenden und Administrierenden über neue oder veränderte Sicherheitsvorgaben für E-Mail-Anwendungen informieren. Die E-Mail-Sicherheitsrichtlinie SOLLTE konform zu den geltenden übergeordneten Sicherheitsrichtlinien der Institution sein. Die Institution SOLLTE prüfen, ob die Sicherheitsrichtlinie korrekt angewendet wird.

Die E-Mail-Sicherheitsrichtlinie für Benutzende SOLLTE vorgeben,

- welche Zugriffsrechte es gibt,
- wie E-Mails auf gefälschte Absendeadressen überprüft werden,
- wie sich übermittelte Informationen absichern lassen,
- wie die Integrität von E-Mails überprüft werden soll,
- welche offenen E-Mail-Verteiler verwendet werden dürfen,
- ob E-Mails privat genutzt werden dürfen,
- wie mit E-Mails und Postfächern ausscheidender Personen umgegangen werden soll,
- ob und wie Webmail-Dienste genutzt werden dürfen,
- wer für Gruppenpostfächer zuständig ist,
- wie mit Datei-Anhängen umgegangen werden soll und
- ob Benutzende die HTML-Darstellung von E-Mails aktivieren dürfen.

Die E-Mail-Sicherheitsrichtlinie SOLLTE ergänzend für die Administrierenden die Einstellungsoptionen der E-Mail-Anwendungen beinhalten, außerdem die Vorgaben für mögliche Zugriffe von anderen Servern auf einen E-Mail-Server. Auch Angaben zu berechtigten Zugriffspunkten, von denen aus auf einen E-Mail-Server zugegriffen werden darf, SOLLTEN in der Richtlinie enthalten sein.

Die E-Mail-Sicherheitsrichtlinie SOLLTE den Umgang mit Newsgroups und Mailinglisten regeln.

APP.5.3.A7 Schulung zu Sicherheitsmechanismen von E-Mail-Clients für Benutzende (S)

Die Institution SOLLTE das Personal darüber aufklären, welche Risiken entstehen, wenn E-Mail-Anwendungen benutzt werden und wie sicher mit E-Mails umgegangen werden kann. Dies SOLLTE zusätzlich zur allgemeinen Schulung und Sensibilisierung geschehen. Die Institution SOLLTE zu den Gefahren sensibilisieren, die entstehen können, wenn E-Mail-Anhänge geöffnet werden. Die Schulungen SOLLTEN ebenfalls darauf eingehen, wie E-Mails von gefälschten Absendeadressen erkannt werden können.

Die Institution SOLLTE davor warnen, an E-Mail-Kettenbriefen teilzunehmen oder zu viele Mailinglisten zu abonnieren.

APP.5.3.A8 Umgang mit Spam durch Benutzende (S) [Benutzende]

Grundsätzlich SOLLTEN die Benutzenden alle Spam-E-Mails ignorieren und löschen. Die Benutzenden SOLLTEN auf unerwünschte E-Mails nicht antworten. Sie SOLLTEN Links in diesen E-Mails nicht folgen. Falls die Institution über ein zentrales Spam-Management verfügt, SOLLTEN die Benutzenden Spam-E-Mails an dieses weiterleiten und die E-Mails danach löschen.

APP.5.3.A9 Erweiterte Sicherheitsmaßnahmen auf dem E-Mail-Server (S)

Die E-Mail-Server einer Institution SOLLTEN eingehende E-Mails mittels des Sender Policy Framework (SPF) und mit Hilfe von DomainKeys Identified Mail (DKIM) überprüfen. Die Institution SOLLTE selbst DKIM und SPF einsetzen, um von ihr versendete E-Mails zu authentisieren.

Wird SPF verwendet, SOLLTEN alle sendeberechtigten E-Mail-Server für eine Domain im SPF-Eintrag angegeben werden. Der SPF-Eintrag SOLLTE den "-all" Parameter enthalten. Der Softfail-Parameter („~“) SOLLTE nur zu Testzwecken verwendet werden.

Die Institution SOLLTE Domain-based Message Authentication, Reporting and Conformance (DMARC) nutzen, um festzulegen, wie von ihr versendete E-Mails durch den empfangenden E-Mail-Server überprüft werden sollen. DMARC-Einträge SOLLTEN vorgeben, dass E-Mails im Fehlerfall abgewiesen werden. DMARC-Reporte SOLLTEN regelmäßig ausgewertet werden. Die Institution SOLLTE festlegen, ob DMARC-Reporte über empfangene E-Mails an andere Institutionen versendet werden.

Die Institution SOLLTE die E-Mail-Kommunikation über DANE und MTA-STS absichern.

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.5.3.A10 Ende-zu-Ende-Verschlüsselung und Signatur (H)

Die Institution SOLLTE eine Ende-zu-Ende-Verschlüsselung sowie digitale Signaturen für E-Mails einsetzen. Es SOLLTEN nur Protokolle zur Verschlüsselung und Signatur genutzt werden, die dem aktuellen Stand der Technik entsprechen.

APP.5.3.A11 Einsatz redundanter E-Mail-Server (H)

Die Institution SOLLTE redundante E-Mail-Server betreiben. Die redundanten E-Mail-Server SOLLTEN mit geeigneter Priorität in den MX-Records der betroffenen Domains hinterlegt werden. Die Institution SOLLTE festlegen, wie E-Mails zwischen den E-Mail-Servern synchronisiert werden.

APP.5.3.A12 Überwachung öffentlicher Block-Listen (H)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, ob die E-Mail-Server der Institution auf öffentlichen Spam- oder Block-Listen aufgeführt sind.

APP.5.3.A13 TLS-Reporting (H)

Die Institution SOLLTE TLS-Reporting einsetzen. Es SOLLTE festgelegt werden, ob TLS-Reports an andere Institutionen versendet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel 13.2.3 Vorgaben für den Betrieb von E-Mail-Diensten.

Das Information Security Forum (ISF) macht in seinem Standard "The Standard of Good Practice for Information Security" im Kapitel CF2.3.3 Vorgaben für den Betrieb von E-Mail-Diensten.

Das National Institute of Standards and Technology (NIST) beschreibt in seinen "Guidelines on Electronic Mail Security" wie E-Mail-Anwendungen sicher betrieben werden können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument "BSI TR-03108 Sicherer E-Mail-Transport" Informationen darüber zur Verfügung, wie E-Mails sicher versendet werden können.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.5.4 Unified Communications und Collaboration (UCC)

1. Beschreibung

1.1. Einleitung

Unified Communications bezeichnet einen Dienst, der verschiedene Kommunikationsdienste in einer Anwendung und in der Regel auch einem Softclient vereint. Damit wird der Anteil der traditionellen Telefonie in der persönlichen digitalen Kommunikation reduziert. Die möglichen Kommunikationswege werden um zusätzliche Dienste wie Video, diverse Formen von Chats und Erreichbarkeitsanzeigen erweitert.

Eine Kommunikationsbeziehung zwischen zwei oder mehr Teilnehmenden wird unabhängig vom benutzten Dienst als Konversation bezeichnet.

Die häufig bei Unified Communications und Collaboration (UCC) genannte Zusammenarbeit (Collaboration) geht noch einen Schritt weiter. Während damit in der Vergangenheit häufig nur Dienste wie Screen Sharing und (digitales) Whiteboarding bezeichnet wurden, stellen UCC-Dienste viele weitere Funktionen zur Verfügung. Insbesondere beim Zusammenarbeiten von Teams hat sich eine Anzahl von Anwendungen etabliert, die häufig als Cloud-Dienst benutzt werden und neben Telefonie, Erreichbarkeitsanzeige, klassischen Chats, Video-Anrufen und Konferenzen auch Team-Chatbereiche sowie gemeinsame Dateiablagen beinhalten. Hinzukommen (offene) Schnittstellen, wodurch zusätzliche Anwendungen integriert werden können, so dass der Gesamtdienst funktional gegebenenfalls sehr umfangreich wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil beim erweiterten Kommunikationsspektrum von UCC-Diensten zu etablieren, ein Bewusstsein für die potenzielle Gefährdungslage dieser Anwendungen zu schaffen und Ansätze zur Vermeidung von Gefährdungen anzubieten.

1.3. Abgrenzung und Modellierung

Der Baustein APP.5.4 *Unified Communications und Collaboration (UCC)* ist auf alle IT-Systeme und Kommunikationsnetze sowie Anwendungen anzuwenden, mit denen UCC-Dienste betrieben werden.

Da UCC über Datennetze betrieben wird, sind zusätzlich zu diesem Baustein die Anforderungen der Bausteine NET.1.1 *Netzarchitektur- und Design* und NET.3.2 *Firewall* zu berücksichtigen.

Da sich der Geltungsbereich von Kommunikationsdiensten durch UCC zunehmend erweitert, gibt es eine besonders große Zahl von Überschneidungen mit anderen Bausteinen.

Dieser Baustein behandelt die folgenden Inhalte:

- die UCC-Dienste sowie Interaktion und Wechselwirkungen unterschiedlicher Dienste
- die (Soft-) Clients, die bereitgestellt werden, um diese Dienste zu benutzen und deren Funktionsumfang
- die zugehörigen Infrastrukturkomponenten, sofern diese nicht bereits durch andere Bausteine abgedeckt sind
- Themen, die sich aus dem (aus Sicht der Benutzenden) fließenden Übergang zwischen der UCC-Umgebung und weiteren Anwendungen ergeben

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Falls über eine dedizierte TK-Anlage telefoniert wird, muss der Baustein NET.4.1 *TK-Anlagen* angewendet werden.
- Für Voice over IP (VoIP) als ein elementarer Dienst bei UCC-Diensten muss der Baustein NET.4.2 *VoIP* angewendet werden.
- Für die zentralen Server sowie diverse Endgeräte und Clients müssen die Bausteine SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Allgemeiner Client* sowie gegebenenfalls spezifische Bausteine angewendet werden.
- Für die zugrundeliegenden Netze muss der Baustein NET.1.1 *Netzarchitektur und -design* angewendet werden.
- Falls UCC-Dienste aus der Cloud bereitgestellt werden, ist der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.
- Um Dateiablagen abzusichern, die im Rahmen der UCC-Dienste bereitgestellt werden, sind insbesondere die Bausteine APP.3.3 *Fileserver* und SYS.1.8 *Speicherlösungen* anzuwenden.

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Der E-Mail-Dienst ist in der Regel nicht Teil der UCC-Dienste. Hier ist der Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* anzuwenden.

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.5.4 *Unified Communications und Collaboration (UCC)* von besonderer Bedeutung.

2.1. Eingeschränkte Verfügbarkeit von UCC-Diensten

UCC-Dienste unterliegen häufig erhöhten Anforderungen an die Verfügbarkeit und gleichzeitig hängt die Funktionstüchtigkeit von UCC-Diensten von weiteren IT-Systemen und Anwendungen ab.

Falls die Datennetze, die von UCC-Diensten verwendet werden, nicht voll funktionsfähig sind, kann das die Verfügbarkeit der UCC-Dienste beeinträchtigen. So können beispielsweise Störungen im Datennetz oder bei der Internetverbindung die Qualität der Kommunikation einschränken, was eine verzögerte Sprachverständigung, Artefakte im Videobild oder den Abbruch der Verbindung verursachen kann.

Abhängigkeiten zwischen kritischen IT-Systemen können auch die Funktionsfähigkeit von weiteren Diensten oder Organisationseinheiten behindern. Wenn beispielsweise UCC als Kommunikationsplattform zwingend erforderlich ist, um das Netz wiederaufzubauen, das Netz aber benötigt wird, damit die UCC-Dienste funktionieren, dann blockieren sich beide und können nicht wiederhergestellt werden.

Häufig werden UCC-Dienste als Cloud-Dienst benutzt oder bei einem Dienstleistungsunternehmen betrieben, wodurch Störungen bei externen Netzen oder beim Dienstleistungsunternehmen zu eingeschränkter Verfügbarkeit der UCC-Dienste führen können. Gleiches gilt für den Authentisierungsdienst, über den sich die Benutzenden an den UCC-Diensten anmelden. Fällt der Authentisierungsdienst aus, können die UCC-Dienste oft nicht mehr verwendet werden.

2.2. Unzureichende Planung von UCC

Wenn UCC nicht so geplant wird, wie es auch tatsächlich benutzt werden soll, kann dies Auswirkungen auf die Funktionalität aller UCC-Dienste haben. Werden UCC-Komponenten verändert oder vermehrt benutzt, z. B. durch eine erhöhte Anzahl von Benutzenden, kann eine ursprünglich geeignete Planung unzureichend werden.

Je nach Bereitstellungsart und benutzten Diensten können sich die Anforderungen der UCC-Komponenten an die Netze stark unterscheiden. Eine auf Sprachkommunikation fokussierte UCC-Komponente im eigenen Netz kann beispielsweise andere Anforderungen an Internet- und WAN-Verbindungen stellen als ein Cloud-Dienst, der auch mobil benutzt werden soll. Werden die Netze nicht so geplant, dass sie UCC-Dienste berücksichtigen, sind die UCC-Dienste nicht ausreichend benutzbar.

Entsprechende Gefährdungen gibt es auch für die zu berücksichtigenden Endgeräte. Besonders die Videokommunikation und die zugehörigen Funktionen stellen zum Teil sehr hohe Anforderungen an die Clients. Insbesondere bei Thin Clients kann dies zu Problemen führen, da UCC-Dienste häufig ganz oder teilweise auf dem Endgerät ausgeführt werden, um Kommunikationsdatenströme zu optimieren. Clients mit unzureichender Rechenleistung können beispielsweise Aussetzer oder Artefakte bei der Videokommunikation bedingen.

2.3. Fehlerhafte Konfiguration von UCC

Eine große Zahl von Funktionen und Diensten bedeutet oft auch eine Vielzahl von Konfigurationsmöglichkeiten. Dabei können Fehlkonfigurationen auftreten.

Benutzende können oder müssen ihre UCC-Clients teilweise selbst konfigurieren. Dies kann Benutzende aufgrund der Vielzahl von Konfigurationsmöglichkeiten überfordern und fehlerhafte Konfigurationen verursachen. Wenn beispielsweise im Büro und im Homeoffice verschiedene Headsets verwendet werden, muss die Konfiguration gegebenenfalls angepasst werden. Fehlkonfigurationen können dazu führen, dass Benutzende in Besprechungen nicht hör- oder sichtbar sind oder selbst keinen Ton hören. Darüber hinaus können ungewollt Informationen preisgegeben werden, wenn Raumsysteme so konfiguriert sind, dass eingehende Kommunikationsanfragen automatisch angenommen werden.

Ebenso können durch ein unzureichendes Identitäts- und Berechtigungskonzept Fehler auftreten, wenn UCC-Dienste konfiguriert werden. Administrierende, die im Rahmen der Einrichtung von neuen Konten ebenfalls zentrale Routing-Einstellungen ändern, können hierdurch eine gravierende Fehlkonfiguration verursachen. Diese kann dazu führen, dass Daten verloren gehen, oder der UCC-Dienst ausfällt.

Zu den Fehlkonfigurationen durch ein unzureichendes Identitäts- und Berechtigungskonzept gehören auch unzureichend eingeschränkte Berechtigungen von externen Teilnehmenden. Können diese beispielsweise unberechtigt auf Inhalte von Konversationen zugreifen, so können Informationen abfließen oder manipuliert werden.

2.4. Unbefugte oder missbräuchliche Benutzung der Administrationsrechte eines UCC-Dienstes

Durch die zugewiesenen Administrationsrechte können Administrierende die UCC-Dienste gegebenenfalls tiefgreifend ändern. Werden Administrationsrechte unbefugt oder missbräuchlich benutzt, kann dies weitreichende Folgen haben. Beispielsweise können Administrationsrechte dazu benutzt werden, um einen privaten Bereich, wie einen Chat oder eine Dateiablage, der ursprünglich nur für einen begrenzten Personenkreis zugänglich war, für alle Benutzenden des UCC-Dienstes freizugeben. Hierdurch können schützenswerte Informationen durch unbefugte Personen eingesehen und gegebenenfalls verändert werden.

Weiterhin können durch vorsätzlich veränderte Routing-Konfigurationen die UCC-Dienste nicht oder nur eingeschränkt zur Verfügung stehen. Falls beispielsweise sämtliche ausgehende Anrufe durch zentrale IT-Systeme blockiert werden, kann der Dienst Telefonie nicht mehr benutzt werden.

2.5. Preisgabe von schützenswerten Informationen

Moderne UCC-Clients verfügen über eine Vielfalt an Funktionen und sind daher für viele Benutzende unübersichtlich. Dies begünstigt Fehlbedienungen, die dazu führen können, dass Informationen nicht regelkonform weitergegeben werden. Wird versehentlich ein falscher Kontakt ausgewählt, erhält dieser gegebenenfalls per Chat ungewollt schützenswerte Informationen. Ein weiteres Szenario ist, ungewollt Informationen bei einer Bildschirmfreigabe preiszugeben, wenn beispielsweise versehentlich der E-Mail-Client statt der vorgesehenen Präsentation freigegeben wird.

Vielen Benutzenden ist nicht bewusst, dass die UCC-Dienste Daten, die beispielsweise innerhalb von privaten Chats gesendet werden, in einer Cloud abspeichern. So können unbewusst Ablagerichtlinien der Institution verletzt werden. Gleiches gilt für Dateien, in denen Konversationen aufgezeichnet wurden.

Teambereiche verfügen zwar in der Regel über einen definierten Kreis von Benutzenden und entsprechende Zugriffsbeschränkungen, jedoch ist vielen Benutzenden nicht bewusst, dass die Zugriffsrechte und Mitgliedschaften nachträglich modifiziert werden können. Dadurch können weitere Personen auf alle zuvor dort abgelegten Dateien zugreifen. Darüber hinaus werden häufig öffentliche Teambereiche erstellt, denen weitere Personen ohne explizite Erlaubnis beitreten können. Dadurch können gegebenenfalls Daten von unberechtigten Personen eingesehen werden. Beispielsweise kann ein Teambereich eines Projekts ausschließlich aus internen Benutzenden bestehen. Teilnehmende laden nun interne Dokumente hoch, da alle Teammitglieder intern sind. Wenn im weiteren Projektverlauf externe Personen in den Bereich eingeladen werden, können sie auf alle bisherigen Dokumente zugreifen.

2.6. Preisgabe von personenbezogenen Informationen

UCC-Dienste erheben an vielen Stellen Daten, die auch anderen Benutzenden angezeigt werden. Dies kann dazu führen, dass personenbezogene Informationen ungewollt preisgegeben werden.

Unter anderem kann die Verfügbarkeit von Benutzenden sichtbar sein. Auch Zeitstempel an Beiträgen in Chats bis hin zu umfangreichen Auswertungen über Gespräche, Aktivitäten oder Inhalte für einzelne Benutzende können Teil einer UCC-Komponente sein. Dabei können sogar Personenprofile durch die UCC-Dienste gebildet werden. Auch Personen ohne erweiterte Berechtigungen erhalten häufig Zugriff auf diese Auswertungen. Dadurch können sie Rückschlüsse auf Arbeitszeiten und -inhalte sowie persönliche Beziehungen anderer Personen ziehen und diese beispielsweise zur Leistungsüberwachung verwenden.

Werden bei mobilem Arbeiten virtuelle Konferenzen benutzt, können ungewollt private Informationen an die Teilnehmenden der Konferenz übermittelt werden. Dazu zählen beispielsweise

Personen, die durch das Videobild laufen, persönliche Gegenstände im Hintergrund einer Videoübertragung oder Geräusche und Stimmen aus dem privaten Umfeld.

2.7. Wechselwirkungen bei UCC-Diensten

UCC-Dienste können untereinander Wechselwirkungen verursachen, welche die Funktionalität einschränken.

Um das Benutzungserlebnis zu verbessern, werden verschiedene Dienste häufig in einer Benutzungsoberfläche verknüpft. Dies kann jedoch zu Abhängigkeiten zwischen den Diensten führen. Wird beispielsweise der Videokonferenzdienst in eine Oberfläche zur Teamkollaboration integriert, kann der Videodienstes nicht mehr verwendet werden, falls die Oberfläche ausfällt.

UCC-Dienste benutzen häufig gemeinsame Ressourcen. Dies kann zu Konflikten führen, welche die Funktionalität beeinträchtigen. Werden Headsets beispielsweise von einer Telefonie- und einer Videokonferenzanwendung gleichzeitig verwendet, können die Headsets durch eine Anwendung blockiert werden und dann nicht mehr für die andere Anwendung zur Verfügung stehen.

Manche Anwendungen haben sehr hohe Ressourcenanforderungen. Wenn mehrere UCC-Dienste gleichzeitig auf einem IT-System ausgeführt werden, kann dies dazu führen, dass der Client überfordert ist und das IT-System ausfällt oder abstürzt. Wenn beispielsweise mehrere Videokonferenzanwendungen parallel im Hintergrund ausgeführt werden, kann die resultierende Auslastung des Arbeitsspeichers den Client stark beeinträchtigen.

2.8. Zugriff auf Applikationen oder Ressourcen durch Freigabe der Steuerung

Werden den Teilnehmenden innerhalb einer Konversation Desktop- oder Bildschirminhalte angezeigt, kann die Steuerung durch den Freigebenden an andere Benutzende übertragen werden. Dies kann jedoch dazu führen, dass der Freigebende die Kontrolle über weitere Handlungen verliert.

Da die Funktion zwar häufig vorhanden ist, in der Regel aber nur selten benutzt wird, sind viele Benutzende mit der Bedienung nicht vertraut, akzeptieren die Freigabe und verlieren dann die Kontrolle über ihren Client. Beispielsweise können Benutzende die Steuerung ihrer Maus freigeben, ohne zu wissen, wie die Freigabe beendet werden kann. Dadurch können Teilnehmende der Konversation möglicherweise auf weitere Anwendungen des Clients zugreifen.

2.9. Vorspiegelung falscher Identitäten

Dadurch, dass neue UCC-Dienste eingeführt werden und Externe neue Möglichkeiten erhalten, Kontakt aufzunehmen, ergeben sich neue Wege für Angreifende, die sich als vertrauenswürdige Kommunikationspartner und -partnerin ausgeben wollen, um so an vertrauliche Informationen zu gelangen.

Die Komplexität von UCC-Diensten erhöht die Wahrscheinlichkeit für Fehlbedienungen oder unbewusste Verletzungen von Sicherheitsrichtlinien durch die Benutzenden. Hyperlinks zu schädlichen Inhalten können beispielsweise geöffnet werden, weil die UCC-Dienste als interne Plattform mit erhöhter Vertrauenswürdigkeit wahrgenommen werden.

Häufig sind sich die Benutzenden nicht darüber bewusst, dass sie auch von unbekannten Externen kontaktiert werden können. Dadurch sind sie anfälliger für Social Engineering, beispielsweise über einen Chat oder eine Einladung zu einer Konversation.

Weiterhin können Angreifende ihre angezeigten Namen, ihre Stimme oder ihr Aussehen manipulieren. Dadurch kann sich zum Beispiel eine externe Person über die vermeintlich interne Kommunikationsplattform als vorgesetzte Person ausgeben, um so vertrauliche Informationen oder Dokumente direkt über den Chat zu erhalten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.5.4 *Unified Communications und Collaboration (UCC)* 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	Keine

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.5.4.A1 Planung von UCC (B)

Es MUSS umfassend und detailliert geplant werden, wie und für welchen Zweck UCC eingesetzt werden soll. Die Planung MUSS insbesondere die Wechselwirkungen der UCC-Dienste berücksichtigen und mindestens folgende Aspekte beinhalten:

- Einsatzzwecke der vorgesehenen UCC-Dienste
- Funktionale Anforderungen an UCC als Gesamtheit und an die einzelnen UCC-Dienste
- Anforderungen zur Absicherung von UCC
- Festlegung zu Informationen und Daten, die über UCC übertragen werden dürfen
- Analyse der Kommunikation und der Abhängigkeiten von UCC-Diensten untereinander
- Produkt- und Dienstauswahl ausgehend von den definierten Anforderungen
- Aufstellen von organisatorischen Regelungen, um die UCC-Dienste zu benutzen

Bei der Planung MUSS berücksichtigt werden, wie UCC in die IT-Infrastruktur der Institution integriert wird. Hierbei MUSS insbesondere betrachtet werden, ob und wie die Systeme der UCC-Dienste innerhalb des Netzes separiert werden sollen und welche Schnittstellen zu weiteren benutzten Anwendungen notwendig sind.

APP.5.4.A2 Berücksichtigung von UCC in der Netzplanung (B)

Bevor UCC-Dienste eingeführt werden, MUSS geprüft werden, ob das Netz die UCC-spezifischen Leistungsparameter erfüllt. Falls die Leistungsparameter nicht erfüllt werden, MUSS festgelegt werden, wie hiermit umgegangen wird.

Sollen UCC-Dienste benutzt werden, SOLLTEN im Rahmen der allgemeinen Netzplanung insbesondere folgende Aspekte berücksichtigt werden:

- Erfüllung der UCC-spezifischen Leistungsparameter wie Paketverlust, Jitter und Latenz
- Netzkapazitäten (Bandbreite) für die festgelegte Benutzung der UCC-Dienste wie Videokonferenzen

- Berücksichtigung von Power over Ethernet (PoE) für stationäre Endgeräte
- Verfügbarkeit von WLAN für mobile Endgeräte

Falls die UCC-Dienste erweitert werden, SOLLTEN diese Aspekte erneut geprüft werden.

APP.5.4.A3 Initiales und regelmäßiges Testen der UCC-Dienste (B)

Für die UCC-Dienste MÜSSEN initial Tests durchgeführt werden, die verifizieren, dass die UCC-Komponenten untereinander und mit anderen UCC-Diensten interferenzfrei funktionieren. Ebenfalls MÜSSEN Tests mit ausgewählten Benutzenden durchgeführt werden, um insbesondere Wechselwirkungen mit anderen Anwendungen zu überprüfen.

Diese Tests SOLLTEN wiederholt werden, wenn die UCC-Dienste erweitert oder verändert werden.

Zusätzlich SOLLTE die Konfiguration der UCC-Dienste in regelmäßigen Abständen auf Plausibilität und Konformität für die festgelegten Einsatzzwecke überprüft werden.

APP.5.4.A4 Deaktivierung nicht benötigter Funktionen und Dienste (B)

UCC-Dienste DÜRFEN NUR mit dem geringsten notwendigen Funktionsumfang betrieben werden. Die verfügbaren Funktionen und Dienste MÜSSEN entsprechend der definierten Einsatzzwecke ausgewählt werden. Dabei MÜSSEN gegebenenfalls auftretende Wechselwirkungen zwischen den verschiedenen Komponenten eines UCC-Dienstes berücksichtigt werden. Außerdem MÜSSEN insbesondere die folgenden Dienste und Funktionen auf Notwendigkeit geprüft und gegebenenfalls deaktiviert oder eingeschränkt werden:

- Speicherung von personenbezogenen Daten durch die UCC-Komponenten
- Zugriff und Verarbeitung von personenbezogenen Daten durch Benutzende und den UCC-Dienst
- Benutzbarkeit von Funktionen wie Chat, Erreichbarkeitsstatus, Dateiablagen oder Team-Bereiche durch externe Teilnehmende
- Senden von Daten und Dateien an externe UCC-Dienste

Konversationsbezogene Log-Daten DÜRFEN NUR in minimal notwendigem Umfang gespeichert werden. Funktionen und Dienste, die auf (dauerhaft) gespeicherte Log-Daten zugreifen, MÜSSEN auf ihre Notwendigkeit geprüft und gegebenenfalls deaktiviert werden.

APP.5.4.A5 Rollen- und Berechtigungskonzept für UCC (B)

Das Rollen- und Berechtigungskonzept MUSS um UCC-spezifische Definitionen von Rollen und Berechtigungen ergänzt werden. Solche Definitionen MÜSSEN sowohl für alle internen Benutzenden als auch für die externen Benutzenden getroffen werden. Es MÜSSEN folgende Aspekte berücksichtigt werden:

- Berechtigungen zur zielgerichteten Benutzung von UCC-Diensten gemäß festgelegter Einsatzzwecke
- Berechtigungen zur Anpassung der Konfiguration von Konversationen
- Berechtigungen für spezielle Funktionen von UCC-Diensten wie Aufzeichnung von Konversationen und Zugriff auf Dateiablagen eines UCC-Dienstes

Darüber hinaus MÜSSEN die Berechtigungen der Konten ebenfalls auf das notwendige Minimum reduziert werden. Dienste, die nur für einen Teil der Benutzenden zur Verfügung stehen, DÜRFEN NICHT für die restlichen Benutzenden zugänglich sein.

Zudem SOLLTEN nur Benutzende mit einer entsprechenden Berechtigung auf Daten wie Aufzeichnungen oder Dateiablagen zugreifen können.

Die Festlegungen MÜSSEN festgehalten, regelmäßig und anlassbezogen geprüft und aktualisiert werden.

APP.5.4.A6 Verschlüsselung von UCC-Daten (B)

Sämtliche Kommunikation über unzureichend vertrauenswürdige Netze MUSS mit sicheren Verfahren verschlüsselt werden, sofern dies durch die jeweilige UCC-Komponente unterstützt wird. Falls eine Verschlüsselung für einzelne UCC-Komponenten oder einzelne Konversationen nicht möglich ist, MUSS die Festlegung, welche Informationen über diese UCC-Komponenten übertragen werden dürfen, geprüft und gegebenenfalls angepasst werden.

Insbesondere MUSS bei anwendungsübergreifender Kommunikation festgelegt werden, für welche Konversationen die Medienströme und die Signalisierung und welche weiteren Daten wie Chat oder Dateitransfer verschlüsselt übertragen werden müssen.

Dateiablagen, die persistente personenbezogene oder vertrauliche Daten enthalten, MÜSSEN mit Hilfe von sicheren Verschlüsselungsmechanismen abgesichert werden. Hierbei MÜSSEN sowohl interne Dateiablagen der UCC-Dienste als auch über Schnittstellen angebundene externe Dateiablagen berücksichtigt werden.

Die Benutzenden MÜSSEN zudem über den Status der Verschlüsselung innerhalb von Konversationen informiert werden.

APP.5.4.A7 Regelungen für eine sichere Benutzung der UCC-Dienste (B)

Konversationen, die mit Hilfe von UCC durchgeführt werden, MÜSSEN abgesichert werden. Hierbei MÜSSEN folgende Aspekte berücksichtigt werden:

- Auswahl der Teilnehmenden entsprechend dem Inhalt der Konversation
- zusätzliche Absicherung von geplanten Konversationen über Mechanismen wie PIN oder ein Passwort
- Zuweisung von Moderationsrechten an ausgewählte Benutzende der einladenden Institution
- Regelungen zum Umgang mit Aufzeichnungen von Konversationen
- Regelungen für Endgeräte, die von mehreren Benutzenden verwendet werden

Die Benutzenden MÜSSEN über Funktionen informiert werden, über die Konversationen abgesichert werden können. Ebenso MÜSSEN die Benutzenden dafür sensibilisiert werden, wie die UCC-Dienste sicher benutzt werden, insbesondere für externe Chats oder Videokonferenzen.

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.5.4.A8 Einsatz eines Session Border Controller am Provider-Übergang (S)

Für die UCC-Kommunikation über eingeschränkt vertrauenswürdige Netze SOLLTE mindestens für Sprachdienste ein Session Border Controller (SBC) am Netzübergang bzw. beim Übergang zum SIP-Provider eingesetzt werden. Der SBC SOLLTE als Verschlüsselungsendpunkt die Signalisierung und die Medienströme terminieren. Der SBC SOLLTE für die Signalisierung und die Medienströme Filterfunktionen unterstützen, die die jeweiligen Konversationen zusätzlich absichern.

APP.5.4.A9 Sichere Konfiguration von UCC (S)

Um UCC sicher zu konfigurieren, SOLLTEN mindestens die folgenden Aspekte berücksichtigt werden:

- Verschlüsselung von Signalisierungs- und Mediendaten auch auf vertrauenswürdigen Übertragungsstrecken
- Absicherung von gespeicherten Daten, insbesondere Festlegung für Zugriffsberechtigung auf Aufzeichnungen von Konversationen

- Einschränkung der zur Verfügung stehenden Dienste auf ausschließlich interne Benutzende
- Einschränkung der Übertragung von Erreichbarkeitsinformationen

Gespeicherte Daten SOLLTEN verschlüsselt werden. Auf gespeicherte Daten SOLLTEN Benutzende nur nach vorheriger Authentisierung zugreifen können.

Der IT-Betrieb SOLLTE sichere Einstellungen vorgeben, die verwendet werden, wenn Konversationen erstellt werden. Für textbasierte Konversationen SOLLTE ein Malware-Schutz aktiviert werden.

Die Umsetzung SOLLTE festgehalten, regelmäßig und anlassbezogen auf Einhaltung der Vorgaben geprüft und angepasst werden.

APP.5.4.A10 Absicherung und Einschränkung von Auswertungen von Inhalten (S)

Die Art einer (automatischen) Auswertung von Konversationsinhalten SOLLTE schon im Vorfeld sorgfältig geprüft werden und ihr Nutzen gegen den Schutzbedarf abgewogen werden. Es SOLLTE die Möglichkeit bestehen, entsprechende Funktionen entweder vollständig oder pro Konversation zu deaktivieren und eine inhaltliche Auswertung der Kommunikation zu verhindern. Besondere Beachtung SOLLTEN KI-Funktionen und die Übertragung von Daten an Onlinedienste erhalten.

Werden Inhalte über den Zweck der Konversation hinausgehend ausgewertet, MUSS dazu auch eine Zustimmung der an der Konversation teilnehmenden Personen eingeholt werden.

Werden während der Auswertung von Konversationen persistente Daten erzeugt, SOLLTEN für diese geeignete Schutzmaßnahmen umgesetzt werden.

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.5.4.A11 Sicherstellung der Verfügbarkeit von Kommunikationsdiensten (H)

Die Verfügbarkeit von UCC-Diensten SOLLTE insbesondere durch folgende technische Maßnahmen sichergestellt werden:

- redundante Auslegung zentraler Server und Dienste
- Benutzung von Call Admission Control (CAC) zur Qualitätssicherung von Telefonie und Video-Diensten
- möglichst autark funktionierende UCC-Dienste

Darüber hinaus SOLLTE bei Cloud-basierten UCC-Diensten der Cloud-Provider sowie der Internet-Provider ausfallsicher an das eigene Netz angebunden werden.

Zudem SOLLTE ein SIP-Provider, der Rufnummern bereitstellt und den Übergang ins öffentliche Telefonnetz bildet, hochverfügbar an das eigene Netz angebunden werden.

Die Verfügbarkeit SOLLTE durch ein Monitoring der UCC-Dienste überwacht werden.

APP.5.4.A12 Einbindung von UCC in die Notfallplanung (H)

Ausgehend von einer Business Impact Analyse SOLLTE geprüft werden, welche UCC-Dienste in der Notfallplanung berücksichtigt werden sollen. Hierbei SOLLTEN in Notfallsituationen für einzelne UCC-Dienste alternative Anwendungen bereitgestellt werden. Insbesondere SOLLTE für die Benutzenden die Erreichbarkeit von wichtigen Diensten wie der Notruf gewährleistet werden.

Zudem SOLLTE ein Notfallplan für die UCC-Dienste erstellt werden, in dem notwendige Konfigurationen sowie Routing-Anpassungen, die über den Telefonie-Provider realisiert werden, behandelt werden.

Ebenso SOLLTE der Wiederanlauf der UCC-Komponenten und -Dienste unter Berücksichtigung der Wechselwirkungen innerhalb der UCC-Dienste festgelegt werden.

APP.5.4.A13 Sichere Administration von SIP-Trunks (H)

Wenn SIP-Trunks administriert werden, SOLLTE für folgende Tätigkeiten ein 4-Augen-Prinzip angewendet werden:

- Änderungen an Routing-Konfigurationen
- Änderungen an Parametern, die im Rahmen von Call Admission Control benutzt werden
- Änderungen hinsichtlich der Verschlüsselung sowohl in Richtung des eigenen Netzes als auch in Richtung des Provider-Netzes
- Änderungen an weiteren sicherheitsrelevanten Konfigurationen wie der lokalen Speicherung von Verbindungsdaten

APP.5.4.A14 Ende-zu-Ende-Verschlüsselung (H)

Für UCC-Kommunikation SOLLTE eine sichere Ende-zu-Ende-Verschlüsselung benutzt werden. Die Ende-zu-Ende-Verschlüsselung SOLLTE sich sowohl auf die Signalisierung als auch auf die Mediendaten von Audio- und Videokommunikation mit zwei oder mehr Teilnehmenden erstrecken.

Bei Konversationen zwischen UCC-Diensten von verschiedenen Herstellenden SOLLTEN die übertragenen Informationen eingeschränkt werden, sofern eine Ende-zu-Ende-Verschlüsselung nach Stand der Technik nicht möglich ist.

APP.5.4.A15 Einschränkung von KI-Funktionen (H)

Die Benutzung von KI-Funktionen SOLLTE deaktiviert oder auf ein Minimum reduziert werden. Ist eine permanente Deaktivierung nicht möglich oder erwünscht, SOLLTE festgelegt werden, dass Benutzende der UCC-Dienste zu Beginn einer Konversation zielgerichtet KI-Funktionen deaktivieren, falls dies möglich ist.

APP.5.4.A16 Einsatz eines SBC an weiteren Netzübergängen (H)

Ergänzend zu einem SBC am Netzübergang zum Provider, SOLLTEN weitere SBC an internen Netzübergängen eingesetzt werden. Hierbei SOLLTEN insbesondere Netzübergänge zwischen Netzsegmenten mit unterschiedlichem Schutzbedarf berücksichtigt werden.

Der SBC SOLLTE sicherstellen, dass die Verschlüsselungsmechanismen an den SBC-gesicherten Netzsegmentübergängen anforderungskonform realisiert werden.

APP.5.4.A17 Einschränkung der Benutzung von UCC-Diensten (H)

Folgende Aspekte SOLLTEN mindestens berücksichtigt werden, um die UCC-Dienste sowie die übertragenen Daten zusätzlich abzusichern:

- Einschränkung der Dienste entsprechend des Schutzbedarfs der übertragenen Informationen
- Benutzung einer Multi-Faktor-Authentisierung für Benutzende
- Deaktivierung von Funktionen für externe Benutzende
- Deaktivierung der Speicherung von Metadaten
- Einschränkung der Sichtbarkeit von kommunikationsbezogenen Daten für Administrierende

Darüber hinaus SOLLTEN zusätzliche technische und organisatorische Vorkehrungen getroffen werden, um Konversationen über die Vergabe von PINs bzw. Passwörtern hinaus abzusichern.

APP.5.4.A18 Einbindung von UCC in ein Sicherheitsmonitoring (H)

Die zentralen UCC-Komponenten SOLLTEN durch ein Sicherheitsmonitoring überwacht werden. Dies SOLLTE mindestens für Komponenten umgesetzt werden, die wie Multipoint Control Units Verschlüsselungsendpunkte realisieren oder die wie SBCs an Vertrauensgrenzen positioniert sind.

Wird für die IT der Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen eingesetzt, SOLLTEN die zentralen UCC-Komponenten hierin eingebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für die Auswahl von Verschlüsselungsverfahren und Schlüssellängen sollte die technische Richtlinie „BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI beachtet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.6 Allgemeine Software

1. Beschreibung

1.1. Einleitung

Dieser Baustein fasst jegliche Software unter dem Begriff Allgemeine Software zusammen, unabhängig davon, ob es sich um eine Textverarbeitung, ein Betriebssystem, eine mobile Kommunikations-App, eine individuell entwickelte Software oder ein verteiltes Content-Management-System handelt.

Dabei durchläuft in der Regel jegliche Software einen Lebenszyklus, der die Planung, Anforderungserhebung, Beschaffung, Software-Tests inklusive Freigabe, Installation in Produktivumgebung, Schulung, Betrieb, Updates und Änderungsmanagement sowie Außerbetriebnahme mitsamt Deinstallation umfasst. Dieser Lebenszyklus kann je nach Anwendungskontext variieren, sodass bei einzelnen Anwendungen noch weitere individuelle Zwischenschritte dazu kommen können und auch der Umfang der einzelnen Schritte schwankt.

Allerdings treten bei den aufgeführten Zwischenschritten immer wiederkehrende Aspekte der Informationssicherheit auf, die auf jegliche Art von Software angewendet werden können.

1.2. Zielsetzung

Der Baustein zeigt auf, welche Sicherheitsanforderungen zu erfüllen sind, damit allgemeine Software über den gesamten Lebenszyklus hinweg sicher eingesetzt werden kann. Übergeordnetes Ziel ist dabei, die Software und die hiermit verarbeiteten Informationen zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.6 *Allgemeine Software* ist grundsätzlich für jede Software, die im Informationsverbund eingesetzt wird, anzuwenden. Ausgenommen hiervon sind Betriebssysteme, die auf geschlossenen Systemen wie IoT-Geräten, Routern, Druckern oder eingebetteten Systemen ausgeführt werden. Häufig wird Software gebündelt ausgeliefert (z. B. Office Suites oder Betriebssysteme mit umfangreich integrierten Boardwerkzeugen) oder um Plug-ins, Add-ons oder vergleichbare erweitert. In solchen Fällen kann der Baustein auf das gesamte Softwarebündel einmal angewendet werden.

Dieser Baustein befasst sich nur mit standardisierten und generischen Verfahrensweisen im Lebenszyklus von Software. Es werden keine konkreten Empfehlungen beschrieben, wie Software im Einzelnen konfiguriert und wie sie durch individuelle Schutzmechanismen auf den eingesetzten IT-

Systemen abgesichert werden soll. Hierzu sind die spezifischen Bausteine der APP-Schicht anzuwenden.

Die Zwischenschritte Freigabe (inklusive Software-Tests) sowie Patch- und Änderungsmanagement werden nicht in diesem Baustein behandelt, sondern in den Bausteinen OPS.1.1.6 *Software-Tests und -Freigaben* sowie OPS.1.1.3 *Patch- und Änderungsmanagement.*

Können Anforderungen an Software nicht von einem fertigen Softwareprodukt erfüllt werden, indem z. B. die Konfiguration angepasst wird, sondern es wird ein individuell entwickeltes Produkt benötigt, dann muss der Baustein APP.7 *Entwicklung von Individualsoftware* ergänzend modelliert werden.

Software und die damit verbundenen Daten müssen häufig auch in Notfällen verfügbar sein. Erste Überlegungen hierzu zeigt der Baustein DER.4 *Notfallmanagement* auf.

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.6 *Allgemeine Software* von besonderer Bedeutung.

2.1. Ungeeignete Auswahl von Software

Für viele Anwendungszwecke und Einsatzmöglichkeiten werden die unterschiedlichsten Software-Lösungen auf dem Markt angeboten. Wird eine unpassende Software, die nicht den Anforderungen der Institution entspricht, ausgewählt, dann kann der Betrieb erheblich gestört werden. Dateiformate könnten zum Beispiel nicht mit bereits eingesetzten Programmen kompatibel sein oder neue Produkte einen zu geringen Funktionsumfang haben. Das kann zu Leistungsverlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

Insbesondere wenn die Software nicht die Sicherheitsanforderungen der Institution erfüllt, könnten die mit der Software verarbeiteten Daten offengelegt oder manipuliert werden, z. B. wenn Login-Funktionen von Anwendungen nicht für die geplante Einsatzumgebung in einem offenen Datennetz konzeptioniert worden sind.

2.2. Offenlegung schützenswerter Informationen durch fehlerhafte Konfiguration

Ist eine Software fehlerhaft konfiguriert, können unbeabsichtigt schützenswerte Informationen offengelegt werden, z. B. wenn nicht benötigte Funktionen noch aktiviert sind, wie Cloud-Backup-Funktionen, die Daten ungewollt in eine Cloud synchronisieren. Hierdurch könnten sensible Daten von unbefugten Dritten eingesehen und offengelegt werden.

Das kann zu finanziellen Einbußen führen oder die Reputation einer Institution schädigen. Zusätzlich könnte die Institution auch gegen geltendes Recht verstoßen, z. B. wenn personenbezogene Daten offengelegt werden.

2.3. Bezug von Software aus unzuverlässiger Quelle

Wird Software aus unzuverlässigen Quellen bezogen, ist nicht sichergestellt, dass eine unveränderte Originalversion der Software eingesetzt wird. Anstelle dessen könnte eine defekte oder kompromittierte Version der Software bezogen worden sein. Dies gilt auch für Erweiterungen, wie Plug-ins oder Add-ons. Wird kompromittierte Software installiert, kann Schadcode in der Institution verteilt werden. Außerdem ist es möglich, dass die Software nicht wie vorgesehen funktioniert. Darüber hinaus kann die Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden.

2.4. Sicherheitslücken durch mangelhafte Wartung

Sicherheitslücken und Software-Schwachstellen können prinzipiell über den gesamten Nutzungszeitraum von Software auftreten. Das kann dazu führen, dass die Informationssicherheit der mit der Software verarbeiten Daten gefährdet ist, indem z. B. Login-Funktionen umgangen oder Verschlüsselungen gebrochen werden können.

Sicherheitslücken und Schwachstellen können insbesondere dann nicht zeitnah behoben werden, wenn kein geeigneter Wartungsvertrag mit dem herstellenden oder anbietenden Unternehmen geschlossen wurde oder die Software schlicht über den Wartungszeitraum hinaus verwendet wird. Auch können Verstöße gegen die Lizenzbestimmungen dazu führen, dass z. B. (Auto-)Update-Mechanismen deaktiviert werden und somit die Software nicht mehr gewartet wird.

2.5. Datenverlust durch fehlerhafte Nutzung von Software

Durch falsch benutzte Software können Mitarbeitende Daten versehentlich löschen oder so verändern, dass diese unbrauchbar werden. Dadurch können ganze Geschäftsprozesse blockiert werden. Auch wenn Funktionen zur Verschlüsselung fehlerhaft benutzt werden, könnten die Daten zwar noch vorhanden sein, aber nicht mehr entschlüsselt werden. In diesem Fall können die Daten nicht mehr oder nur noch mit erhöhtem Aufwand wiederhergestellt werden.

2.6. Mangelhafte Ressourcen für die Ausführung von Software

Falls IT-Systeme über ungenügend Ressourcen verfügen, um die Software auszuführen, kann das die Bearbeitungs- und Reaktionszeit für die Benutzende erheblich erhöhen. Im schlimmsten Fall kann die Software auf solch einem System nicht ausgeführt werden. Das kann Geschäftsprozesse erheblich unterbrechen.

2.7. Nichtbeachtung von Anforderungen der Benutzenden

Unabhängig davon, ob eine Software die funktionalen Anforderungen erfüllt, kann sie von den Benutzenden nicht akzeptiert werden, wenn sie z. B. umständlich und kompliziert zu bedienen ist. Dies kann wiederum dazu führen, dass Benutzende auf alternative Formen der Bearbeitung zurückgreifen und dafür anderweitige IT-Systeme oder Software zweckentfremden. So könnten z. B. private IT-Systeme ohne Abstimmung mit dem IT-Betrieb eingesetzt werden. Diese alternativen Formen der Bearbeitung entstehen dabei selten unter Gesichtspunkten der Informationssicherheit und stellen somit ein erhöhtes Risiko dar.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.6 *Allgemeine Software* 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, Beschaffungsstelle

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.6.A1 Planung des Software-Einsatzes (B) [Fachverantwortliche]

Bevor eine Institution eine (neue) Software einführt, MUSS sie entscheiden,

- wofür die Software genutzt und welche Informationen damit verarbeitet werden sollen,
- wie die Benutzenden bei der Anforderungserhebung beteiligt und bei der Einführung unterstützt werden sollen,
- wie die Software an weitere Anwendungen und IT-Systeme über welche Schnittstellen angebunden wird,
- auf welchen IT-Systemen die Software ausgeführt werden soll und welche Ressourcen zur Ausführung der Software erforderlich sind, sowie
- ob sich die Institution in Abhängigkeit zu einem Hersteller oder einer Herstellerin begibt, wenn sie diese Software einsetzt.

Hierbei MÜSSEN bereits Sicherheitsaspekte berücksichtigt werden. Zusätzlich MUSS die Institution die Zuständigkeiten für fachliche Betreuung, Freigabe und betriebliche Administration schon im Vorfeld klären und festlegen. Die Zuständigkeiten MÜSSEN dokumentiert und bei Bedarf aktualisiert werden.

APP.6.A2 Erstellung eines Anforderungskatalogs für Software (B) [Fachverantwortliche]

Auf Basis der Ergebnisse der Planung MÜSSEN die Anforderungen an die Software in einem Anforderungskatalog erhoben werden. Der Anforderungskatalog MUSS dabei die grundlegenden funktionalen Anforderungen umfassen. Darüber hinaus MÜSSEN die nichtfunktionalen Anforderungen und hier insbesondere die Sicherheitsanforderungen in den Anforderungskatalog integriert werden.

Hierbei MÜSSEN sowohl die Anforderungen von den Fachverantwortlichen als auch vom IT-Betrieb berücksichtigt werden. Insbesondere MÜSSEN auch die rechtlichen Anforderungen, die sich aus dem Kontext der zu verarbeitenden Daten ergeben, berücksichtigt werden.

Der fertige Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen abgestimmt werden.

APP.6.A3 Sichere Beschaffung von Software (B) [Beschaffungsstelle]

Wenn Software beschafft wird, MUSS auf Basis des Anforderungskatalogs eine geeignete Software ausgewählt werden. Die ausgewählte Software MUSS aus vertrauenswürdigen Quellen beschafft werden. Die vertrauenswürdige Quelle SOLLTE eine Möglichkeit bereitstellen, die Software auf Integrität zu überprüfen.

Darüber hinaus SOLLTE die Software mit einem geeigneten Wartungsvertrag oder einer vergleichbaren Zusage des herstellenden oder anbietenden Unternehmens beschafft werden. Diese Verträge oder Zusagen SOLLTEN insbesondere garantieren, dass auftretende Sicherheitslücken und Schwachstellen der Software während des gesamten Nutzungszeitraums zeitnah behoben werden.

APP.6.A4 Regelung für die Installation und Konfiguration von Software (B) [Fachverantwortliche]

Die Installation und Konfiguration der Software MUSS durch den IT-Betrieb so geregelt werden, dass

- die Software nur mit dem geringsten notwendigen Funktionsumfang installiert und ausgeführt wird,
- die Software mit den geringsten möglichen Berechtigungen ausgeführt wird,
- die datensparsamsten Einstellungen (in Bezug auf die Verarbeitung von personenbezogenen Daten) konfiguriert werden sowie
- alle relevanten Sicherheitsupdates und -patches installiert sind, bevor die Software produktiv eingesetzt wird.

Hierbei MÜSSEN auch abhängige Komponenten (unter anderem Laufzeitumgebungen, Bibliotheken, Schnittstellen sowie weitere Programme) mitbetrachtet werden. Der IT-Betrieb MUSS in Abstimmung mit den Fachverantwortlichen festlegen, wer die Software wie installieren darf. Idealerweise SOLLTE Software immer zentral durch den IT-Betrieb installiert werden. Ist es erforderlich, dass die Software (teilweise) manuell installiert wird, dann MUSS der IT-Betrieb eine Installationsanweisung erstellen, in der klar geregelt wird, welche Zwischenschritte zur Installation durchzuführen und welche Konfigurationen vorzunehmen sind.

Darüber hinaus MUSS der IT-Betrieb regeln, wie die Integrität der Installationsdateien überprüft wird. Falls zu einem Installationspaket digitale Signaturen oder Prüfsummen verfügbar sind, MÜSSEN mit diesen die Integrität überprüft werden.

Sofern erforderlich, SOLLTE der IT-Betrieb eine sichere Standardkonfiguration der Software festlegen, mit der die Software konfiguriert wird. Die Standardkonfiguration SOLLTE dokumentiert werden.

APP.6.A5 Sichere Installation von Software (B)

Software MUSS entsprechend der Regelung für die Installation auf den IT-Systemen installiert werden. Dabei MÜSSEN ausschließlich unveränderte Versionen der freigegebenen Software verwendet werden.

Wird von diesen Anweisungen abgewichen, MUSS dies durch Vorgesetzte und den IT-Betrieb genehmigt werden und entsprechend dokumentiert 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.6.A6 Berücksichtigung empfohlener Sicherheitsanforderungen (S)

Die Institution SOLLTE die nachfolgenden Sicherheitsanforderungen im Anforderungskatalog für die Software berücksichtigen:

- Die Software SOLLTE generelle Sicherheitsfunktionen wie Protokollierung und Authentifizierung umfassen, die im Anwendungskontext erforderlich sind.
- Die Software SOLLTE es ermöglichen, die Härtungsfunktionen der Einsatzumgebung zu nutzen. Hierbei SOLLTEN insbesondere die Härtungsfunktionen des geplanten Betriebssystems und der geplanten Ausführungsumgebung berücksichtigt werden.
- Wenn durch die Software Informationen über ungesicherte, öffentliche Netze übertragen werden, dann SOLLTE die Software sichere Verschlüsselungsfunktionen einsetzen, die dem Stand der Technik entsprechen. Darüber hinaus SOLLTEN die übertragenen Daten auf Integrität überprüft werden, indem Prüfsummen oder digitale Signaturen eingesetzt werden.
- Verwendet die Software Zertifikate, dann SOLLTE sie die Möglichkeit bieten, die Zertifikate transparent darzustellen. Zudem SOLLTE es möglich sein, Zertifikate zu sperren, ihnen das Vertrauen zu entziehen oder eigene Zertifikate zu ergänzen.

Die sich aus den Sicherheitsanforderungen ergebenden Funktionen der Software SOLLTEN im Betrieb verwendet werden.

APP.6.A7 Auswahl und Bewertung potentieller Software (S) [Fachverantwortliche, Beschaffungsstelle]

Anhand des Anforderungskatalogs SOLLTEN die am Markt erhältlichen Produkte gesichtet werden. Sie SOLLTEN mithilfe einer Bewertungsskala miteinander verglichen werden. Danach SOLLTE untersucht werden, ob die Produkte aus der engeren Wahl die Anforderungen der Institution erfüllen. Gibt es mehrere Alternativen für Produkte, SOLLTEN auch die Akzeptanz der Benutzenden und der zusätzliche Aufwand für z. B. Schulungen oder die Migration berücksichtigt werden. Fachverantwortliche SOLLTEN gemeinsam mit dem IT-Betrieb anhand der Bewertungen und Testergebnisse ein geeignetes Softwareprodukt auswählen.

APP.6.A8 Regelung zur Verfügbarkeit der Installationsdateien (S)

Der IT-Betrieb SOLLTE die Verfügbarkeit der Installationsdateien sicherstellen, um die Installation reproduzieren zu können. Hierzu SOLLTE der IT-Betrieb

- die Installationsdateien geeignet sichern oder
- die Verfügbarkeit der Installationsdateien durch die Bezugsquelle (z. B. App-Store) sicherstellen.

Zusätzlich SOLLTE sichergestellt werden, dass Software reproduzierbar konfiguriert werden kann. Hierzu SOLLTEN die Konfigurationsdateien gesichert werden. Alternativ SOLLTE geeignet dokumentiert werden, wie die Software konfiguriert wird.

Diese Regelung SOLLTE in das Datensicherungskonzept der Institution integriert werden.

APP.6.A9 Inventarisierung von Software (S)

Software SOLLTE inventarisiert werden. In einem Bestandsverzeichnis SOLLTE dokumentiert werden, auf welchen Systemen die Software unter welcher Lizenz eingesetzt wird. Bei Bedarf SOLLTEN zusätzlich die sicherheitsrelevanten Einstellungen miterfasst werden. Software SOLLTE nur mit Lizenzen eingesetzt werden, die dem Einsatzzweck und den vertraglichen Bestimmungen entsprechen. Die Lizenz SOLLTE den gesamten vorgesehenen Benutzungszeitraum der Software abdecken.

Wird von einer Standardkonfiguration abgewichen, SOLLTE dies dokumentiert werden. Das Bestandsverzeichnis SOLLTE anlassbezogen durch den IT-Betrieb aktualisiert werden, insbesondere wenn Software installiert wird.

Das Bestandsverzeichnis SOLLTE so aufgebaut sein, dass bei Sicherheitsvorfällen eine schnelle Gesamtübersicht mit den notwendigen Details ermöglicht wird.

APP.6.A10 Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software (S)

Die Institution SOLLTE die Regelungen, die festlegen, wie die Software eingesetzt und betrieben wird, in einer Sicherheitsrichtlinie zusammenfassen. Die Richtlinie SOLLTE allen relevanten Verantwortlichen, Zuständigen und Mitarbeitenden der Institution bekannt sein und die Grundlage für ihre Arbeit und ihr Handeln bilden. Inhaltlich SOLLTE die Richtlinie auch ein Benutzenden-Handbuch umfassen, dass erläutert, wie die Software zu benutzen und zu administrieren ist.

Es SOLLTE regelmäßig und stichprobenartig überprüft werden, ob die Mitarbeitenden sich an die Richtlinie halten. Die Richtlinie SOLLTE regelmäßig aktualisiert werden.

APP.6.A11 Verwendung von Plug-ins und Erweiterungen (S)

Es SOLLTEN nur unbedingt notwendige Plug-ins und Erweiterungen installiert werden. Werden Erweiterungen eingesetzt, SOLLTE die Software die Möglichkeit bieten, Erweiterungen zu konfigurieren und abzuschalten.

APP.6.A12 Geregelte Außerbetriebnahme von Software (S) [Fachverantwortliche]

Wenn Software außer Betrieb genommen wird, SOLLTE der IT-Betrieb mit den Fachverantwortlichen regeln, wie dies im Detail durchzuführen ist. Ebenfalls SOLLTE geregelt werden, wie die Benutzenden hierüber zu informieren sind. Hierbei SOLLTE geklärt werden, ob die funktionalen Anforderungen fortbestehen (z. B. zur Bearbeitung von Fachaufgaben). Ist dies der Fall, dann SOLLTE geregelt werden, wie die benötigten Funktionen der betroffenen Software weiter verfügbar sein werden.

APP.6.A13 Deinstallation von Software (S)

Wird Software deinstalliert, SOLLTEN alle angelegten und nicht mehr benötigten Dateien entfernt werden. Alle Einträge in Systemdateien, die für das Produkt vorgenommen wurden und nicht länger benötigt werden, SOLLTEN rückgängig gemacht werden.

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.6.A14 Nutzung zertifizierter Software (H)

Bei der Beschaffung von Software SOLLTE festgelegt werden, ob Zusicherungen des herstellenden oder anbietenden Unternehmens über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden können. Ist dies nicht der Fall, SOLLTE eine Zertifizierung der Anwendung z. B. nach Common Criteria als Entscheidungskriterium herangezogen werden. Stehen mehrere Produkte zur Auswahl, SOLLTEN insbesondere dann Sicherheitszertifikate berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.14 „Security requirements of information systems“ Anforderungen an die Informationssicherheit von IT-Systemen, die auch bei der Auswahl und dem Einsatz von Software berücksichtigt werden sollten.

Die Common Criteria for Information Technology Security Evaluation (CC) stellen die Basis für international anerkannte Produktzertifizierungen dar. Eine CC-Zertifizierung kann somit als Nachweis für die Informationssicherheit eines Softwareproduktes herangezogen werden.

Das National Institute of Standardisation and Technology formuliert in der NIST Special Publication 800-53 im Appendix F „Family System and Service Acquisition“ unter anderem Anforderungen an die Anschaffung von IT-Produkten, hierunter auch Software.

Das Information Security Forum (ISF) stellt in seinem Standard „The Standard of Good Practice for Information Security“ in dem Kapitel „Business Application Management“ unter anderem Best Practices zur Absicherung von Software vor.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.7 Entwicklung von Individualsoftware

1. Beschreibung

1.1. Einleitung

Viele Institutionen stehen vor Herausforderungen, die sie nicht mehr hinreichend mit unangepasster Software lösen können. Die mit diesen Herausforderungen verbundenen Aufgabenstellungen bedürfen häufig Softwarelösungen, die auf die individuellen Bedürfnisse der Institutionen zugeschnitten sind. Im Folgenden werden diese Softwarelösungen als Individualsoftware bezeichnet. Hierzu können einerseits Basislösungen, die aus einer Grundmenge an typischen Funktionen bestehen, eingesetzt und individualisiert werden. Die Grundfunktionen werden hierbei für den individuellen Einsatzzweck der Institution angepasst und um individuell benötigte Funktionen erweitert. Gängige Beispiele hierfür sind IT-Anwendungen wie ERP- (Enterprise Resource Planning), CMS- (Content Management Systeme) oder IDM-Systeme (Identity Management). Individualsoftware kann auch vollständig neu von der Institution selbst oder von Dritten entwickelt werden. Hierzu gehören Anwendungen zur Geschäftsprozesssteuerung oder individuell angepasste Fachanwendungen, wie Personalverwaltungssoftware, Verfahren zur Verwaltung von Sozialdaten oder Meldedaten.

Von essentieller Bedeutung ist es hierbei, dass bereits bei der Planung und Konzeptionierung der Individualsoftware auch die benötigten Sicherheitsfunktionen bedacht werden und die Informationssicherheit in dem gesamten Lebenszyklus der Individualsoftware berücksichtigt wird. Fehler in der Planung oder fehlende Sicherheitsfunktionen können im laufenden Betrieb nicht oder nur mit hohem zusätzlichem Aufwand ausgeglichen werden.

Individualsoftware wird dabei in der Regel im Rahmen eines Projektes entwickelt. Hierzu haben sich die unterschiedlichsten Vorgehens- bzw. Projektmanagementmodelle etabliert. Während klassische, lineare Vorgehensmodelle, wie der Wasserfallprozess, sehr gut zu Projekten mit zu Beginn feststehenden Anforderungen passen, ermöglichen agile Vorgehensmodelle, wie Scrum, Individualsoftware iterativ und inkrementell zu entwickeln. Agile Vorgehensmodell können sich somit besser an verändernde Gegebenheiten anpassen, insbesondere wenn zu Beginn noch nicht alle Anforderungen feststehen. Allerdings bieten sie nicht dieselbe Kalkulationssicherheit wie lineare Vorgehensmodelle und passen auch in einigen Fällen nicht zu den klassischen Strukturen der Beschaffungsprozesse, die auf ein lineares Vorgehen ausgerichtet sind.

1.2. Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, welche grundlegenden Sicherheitsanforderungen bei der Planung und Entwicklung von Individualsoftware zu berücksichtigen sind.

1.3. Abgrenzung und Modellierung

Der Baustein APP.7 *Entwicklung von Individualsoftware* ist für jede Entwicklung einer Individualsoftware einmal anzuwenden.

Aspekte zur Planung, Konzeption und Einsatz von Individualsoftware, wie benötigte Sicherheitsfunktionen festzulegen oder Individualsoftware außer Betrieb zu nehmen, werden im Baustein APP.6 *Allgemeine Software* behandelt. Er ist daher immer zusammen mit diesem Baustein anzuwenden.

Wenn Software entwickelt wird, liegt sehr häufig ein auftragnehmendes und auftraggebendes Verhältnis vor. Im IT-Grundschutz spiegelt sich dieser Sachverhalt wider, indem der Baustein APP.7 *Entwicklung von Individualsoftware* die auftragsgebende Seite und der Baustein CON.8 *Software-Entwicklung* die auftragnehmende Seite behandeln.

Die Freigabe und Tests von Individualsoftware wird im Baustein OPS.1.1.6 *Software-Tests und -Freigaben* behandelt.

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.7 *Entwicklung von Individualsoftware* von besonderer Bedeutung.

2.1. Unzulängliche vertragliche Regelungen mit externen Dienstleistenden

Aufgrund von unzulänglichen vertraglichen Regelungen mit externen Dienstleistenden können vielfältige und schwerwiegende Sicherheitsprobleme auftreten. Dies gilt insbesondere, wenn Anwendungen erstellt, eingeführt oder gewartet werden. Sind Aufgaben, Leistungsparameter oder der Aufwand ungenügend oder missverständlich beschrieben, können Sicherheitsmaßnahmen möglicherweise aus Unkenntnis oder aufgrund mangelnder Qualifizierung oder fehlender Ressourcen nicht umgesetzt werden. Dies kann viele negative Auswirkungen nach sich ziehen, etwa wenn regulatorische Anforderungen und Pflichten nicht erfüllt werden, Auskunftspflichten und Gesetze nicht eingehalten werden oder keine Verantwortung übernommen wird, weil Kontroll- und Steuerungsmöglichkeiten fehlen.

2.2. Software-Konzeptionsfehler

Werden Anwendungen, Programme und Protokolle konzeptioniert, können sicherheitsrelevante Konzeptionsfehler entstehen. Diese ergeben sich häufig daraus, dass Anwendungsmodule und Protokolle, die für einen bestimmten Zweck vorgesehen sind, in anderen Einsatzszenarien wiederverwendet werden. Sind dann andere Sicherheitsvorgaben relevant, kann dies zu massiven Sicherheitsproblemen führen, zum Beispiel wenn Anwendungsmodule und Protokolle, die eigentlich für abgeschottete betriebliche Umgebungen vorgesehen sind, an das Internet angebunden werden.

2.3. Undokumentierte Funktionen

Viele Anwendungen enthalten vom herstellenden Unternehmen eingebaute, undokumentierte Funktionen, häufig für die Entwicklung oder zum Support der Anwendung. Diese sind den Benutzenden meistens nicht bekannt. Undokumentierte Funktionen sind dann problematisch, wenn sie es erlauben, dass wesentliche Sicherheitsmechanismen umgangen werden, z. B. zum Zugriffsschutz. Dies kann die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten erheblich beeinträchtigen.

2.4. Fehlende oder unzureichende Sicherheitsmaßnahmen in Anwendungen

Sicherheitsmechanismen oder Sicherheitsfunktionen sollen in der Anwendung sicherstellen, dass bei der Verarbeitung von Informationen die Vertraulichkeit, Integrität und Verfügbarkeit im benötigten Maße gewährleistet werden können. Häufig steht bei der Entwicklung einer Anwendung aber die fachliche Funktionalität oder der Zeit- und Kostenrahmen im Vordergrund. So können wichtige Sicherheitsmechanismen zu schwach ausgeprägt sein, sodass sie einfach umgangen werden können oder sogar ganz fehlen.

2.5. Mangelhafte Steuerung der Software-Entwicklung

Wird die Software-Entwicklung vom Auftraggebenden nicht hinreichend gesteuert, bestehen eine Reihe von Gefahren, wie z. B.:

- Es können geforderte Sicherheitsfunktionen fehlen oder nur unzureichend implementiert werden. Hieraus können sich vielfältige Risiken ergeben, die die Verfügbarkeit, Vertraulichkeit und Integrität der mit der Individualsoftware verarbeiteten Daten gefährden.
- Das Entwicklungsprojekt kann sich zeitlich verzögern, sodass die Individualsoftware nicht rechtzeitig verfügbar ist.
- Prioritäten können falsch gesetzt werden, indem z. B. nachrangig benötigte Funktionen umfangreich entwickelt werden und dringend benötigte Sicherheitsfunktionen nur rudimentär implementiert werden. Auch hieraus können Projektverzögerungen und vielseitige Sicherheitsrisiken entstehen.

2.6. Beauftragung ungeeigneter Software-Entwickelnder

Werden ungeeignete Software-Entwickelnde beauftragt, können daraus unterschiedliche Gefährdungen entstehen:

- Aufgrund fehlender fachlicher Expertise, z. B. in der verwendeten Programmiersprache, in den eingesetzten Frameworks oder der geplanten technischen Einsatzumgebung, kann die Software viele vermeidbare Sicherheitslücken umfassen.
- Fehlende Kenntnisse im Bereich des Projektmanagements und Requirements Engineering können zu Reibungsverlusten in Abstimmungsprozessen und somit zu erheblichen Verzögerungen führen. Auch können deswegen Schwerpunkte falsch gesetzt werden und so wesentliche Sicherheitsfunktionen nicht mit der erforderlichen Priorität implementiert werden. Ungeeignete Software-Entwickelnde können beispielsweise aufgrund zu knapper, unrealistischer Kostenkalkulationen beauftragt werden. Auch Fehler, missverständliche Anforderungen und falsche Zielvorstellungen in Ausschreibungen können dazu führen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.7 *Entwicklung von Individualsoftware* 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	Fachverantwortliche
Weitere Zuständigkeiten	Beschaffungsstelle, IT-Betrieb

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.7.A1 Erweiterung der Planung des Software-Einsatzes um Aspekte von Individualsoftware (B)

Die Planung des Software-Einsatzes MUSS um Aspekte von Individualsoftware ergänzt werden, indem definiert wird,

- wer dafür zuständig ist, die Software-Entwicklung bzw. den Auftragnehmenden zu steuern und zu koordinieren, sowie
- in was für einen organisatorischen Rahmen die Software zu entwickeln ist (Projektmanagementmodell).

Individualsoftware SOLLTE im Rahmen eines Entwicklungsprojektes entwickelt werden. Das Entwicklungsprojekt sollte anhand eines Ablaufplans zeitlich grob geplant werden.

APP.7.A2 Festlegung von Sicherheitsanforderungen an den Prozess der Software-Entwicklung (B)

Die Institution MUSS klare Anforderungen an den Prozess der Software-Entwicklung definieren. Aus den Anforderungen MUSS hervorgehen, in was für einer Umgebung die Software entwickelt werden darf und welche technischen und organisatorischen Maßnahmen von Seiten der beauftragten Software-Entwickelnden umzusetzen sind.

APP.7.A3 Festlegung der Sicherheitsfunktionen zur Systemintegration (B) [IT-Betrieb]

Der IT-Betrieb und die zuständigen Fachverantwortlichen MÜSSEN Anforderungen an die technische Einsatzumgebung der geplanten Individualsoftware erstellen und mit der Software-Entwicklung abstimmen. Aus den Anforderungen MUSS klar hervorgehen:

- auf was für einer Hardware-Plattform,
- auf was für einer Software-Plattform (inklusive gesamten Software-Stack),
- mit welchen zur Verfügung stehenden Ressourcen (z. B. CPU-Cluster oder Arbeitsspeicher),
- mit welchen Schnittstellen mit anderen IT-Systemen oder Anwendungen sowie

- mit welchen sich hieraus ergebenen Sicherheitsfunktionen

die Anwendung eingesetzt werden soll. Schnittstellen mit anderen IT-Systemen SOLLTEN in standardisierten technischen Formaten modelliert und definiert werden.

APP.7.A4 Anforderungsgerechte Beauftragung (B) [Beschaffungsstelle]

Wird Individualsoftware durch die eigene Institution entwickelt oder extern beauftragt, dann MÜSSEN neben den bestehenden rechtlichen und organisatorischen Vorgaben insbesondere

- der Anforderungskatalog (siehe hierzu APP.6 *Allgemeine Software*),
- die Sicherheitsanforderungen an den Prozess der Software-Entwicklung, sowie
- die Sicherheitsfunktionen zur Systemintegration

als Grundlage zur Software-Entwicklung 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.7.A5 Geeignete Steuerung der Anwendungsentwicklung (S)

Bei der Entwicklung von Individualsoftware SOLLTE ein geeignetes Steuerungs- und Projektmanagementmodell verwendet werden. Hierbei SOLLTE das ausgewählte Modell mit dem Auftragnehmenden abgestimmt werden. Bei der Steuerung SOLLTE es berücksichtigt werden.

Es SOLLTE insbesondere berücksichtigt werden, dass das benötigte Personal ausreichend qualifiziert ist. Alle relevanten Phasen SOLLTEN während des Lebenszyklus der Software abgedeckt werden. Außerdem SOLLTE es ein geeignetes Entwicklungsmodell, ein Risikomanagement sowie Qualitätsziele enthalten.

APP.7.A6 Dokumentation der Anforderungen an die Individualsoftware (S)

Die Anforderungen aus den Anforderungskatalog, die Sicherheitsanforderungen an den Prozess der Software-Entwicklung, sowie die Sicherheitsfunktionen zur Systemintegration SOLLTEN umfassend dokumentiert werden. Insbesondere SOLLTE ein Sicherheitsprofil für die Anwendung erstellt werden. Dieses SOLLTE den Schutzbedarf der zu verarbeitenden Daten und Funktionen dokumentieren. Die Dokumentation mitsamt Sicherheitsprofil SOLLTE den Entwickelnden zur Software-Entwicklung zur Verfügung gestellt werden.

Die Dokumentation SOLLTE bei Änderungen an der Individualsoftware sowie bei funktionalen Updates aktualisiert werden.

APP.7.A7 Sichere Beschaffung von Individualsoftware (S)

Das Entwicklungsprojekt SOLLTE im Rahmen des hierfür bestens geeigneten Projektmanagementmodells beauftragt werden. Sicherheitsaspekte SOLLTEN dabei bereits bei der Ausschreibung und Vergabe berücksichtigt werden, sodass

- einerseits nur geeignete Auftragnehmende beauftragt werden,
- andererseits aber keine weitreichenden Rückschlüsse auf die Sicherheitsarchitektur durch die öffentlich verfügbaren Informationen möglich sind.

In der Institution SOLLTEN definierte Prozesse und festgelegte Kontaktpersonen existieren, die sicherstellen, dass die jeweiligen Rahmenbedingungen berücksichtigt werden.

APP.7.A8 Frühzeitige Beteiligung der Fachverantwortlichen bei entwicklungsbegleitenden Software-Tests (S)

Fachverantwortliche SOLLTEN schon vor der endgültigen Abnahme frühzeitig an entwicklungsbegleitenden Tests der Software-Entwickelnden beteiligt werden. Dies SOLLTE in Abstimmung mit dem Auftragnehmenden bereits initial im Projektablaufplan berücksichtigt werden.

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.7.A9 Treuhänderische Hinterlegung (H)

Für institutionskritische Anwendungen SOLLTE geprüft werden, ob diese gegen Ausfall des herstellenden Unternehmens abgesichert werden. Dafür SOLLTEN nicht zum Lieferumfang der Anwendung gehörende Materialien und Informationen treuhänderisch hinterlegt werden, etwa bei einer Escrow-Agentur. Dokumentierter Code, Konstruktionspläne, Schlüssel oder Passwörter SOLLTEN dazu gehören. Die Pflichten der Escrow-Agentur zur Hinterlegung und Herausgabe SOLLTEN vertraglich geregelt werden. Es SOLLTE geklärt werden, wann das Hinterlegte an wen herausgegeben werden darf.

APP.7.A10 Beauftragung zertifizierter Software-Entwicklungsunternehmen (H)

Werden besonders sicherheitskritische Anwendungen entwickelt, SOLLTEN hierzu zertifizierte Software-Entwicklungsunternehmen beauftragt werden. Die Zertifizierung SOLLTE Sicherheitsaspekte für relevante Aspekte der Software-Entwicklung umfassen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt

- in der Norm ISO/IEC 12207:2008, „System and software engineering - Software life cycle process“ einen Überblick über alle Bestandteile des Lebenszyklus einer Software,
- in der Norm ISO/IEC 15408-2:2008, „Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components“ einen Überblick über die Möglichkeiten der Systemabsicherung und
- in der Norm ISO/IEC 27001:2013, „Information technology - Security technigues - Information security management systems - Requirements“ im Annex A, A.14 System acquisition, development and maintenance“ Anforderungen an die System-Entwicklung und den -betrieb.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in der „Area BA Business Application Management“ Anforderungen an das Management von Business-Anwendungen.

Das National Institute of Standards and Technology stellt in der „NIST Special Publication 800-53“ im Apendix F-SA „Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity“ weitergehende Anforderungen an den Umgang mit Individualsoftware.