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 optional angehängten Dateien an andere Personen zu versenden. Dazu benötigen Benutzer eine E-Mail-Adresse.

Um E-Mail-Anwendungen nutzen zu können, werden E-Mail-Server benötigt, die elektronische Nachrichten empfangen und versenden. In der Regel rufen E-Mail-Clients 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 Angreifern.

Auch E-Mail-Clients stehen im Fokus der Angreifer. 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 diese 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-Server und -Clients. 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.

2. Gefährdungslage

Folgende spezifische 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 kann 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 fehlerhafte Einstellungen und 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 dazuführen, 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 E-Mail-Servern in anderen Institutionen ermöglichen, zu überprüfen, ob eine E-Mail tatsächlich vom angegebenen Absender stammt. Außerdem kann ein falsch eingestellter E-Mail-Server von Angreifern dazu missbraucht werden, um Spam-E-Mails zu versenden.

2.3. Unzuverlässigkeit von E-Mail

Über E-Mail-Dienste 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 Empfängeradresse nicht

korrekt angegeben wurde. Im schlimmsten Fall können vertrauliche Informationen an falsche Empfänger gesendet worden sein.

2.4. Schadsoftware in E-Mails

Es gibt verschiedene Wege, auf denen ein Angreifer Schadsoftware mit Hilfe von E-Mails verbreiten 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 Benutzer die Anhänge öffnen, 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 von Angreifern dazu eingesetzt, um vertrauliche Informationen zu erhalten oder Benutzer zu anderem schädlichen Verhalten zu verleiten. Beispielsweise kann ein Angreifer eine E-Mail senden, die vermeintlich von einem Vorgesetzten des Benutzers stammt und darin Anweisungen erteilen, 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 eines eigentlich vertrauenswürdigen Anbieters dazu auffordert, Zugangsdaten auf einer Webseite einzugeben (Phishing). Die so gewonnenen Zugangsdaten können dann vom Angreifer für weitere Aktionen verwendet werden.

Verstärkt wird die Gefahr von Social Engineering, wenn Benutzer nicht regelmäßig zu diesen Gefährdungen geschult und sensibilisiert werden.

2.6. Mitlesen und Manipulieren von E-Mails

E-Mails werden in der Regel unverschlüsselt und ohne Signatur versendet. Deswegen kann ein Angreifer E-Mails mitlesen und sogar beliebig verändern. Auf diesem Weg kann er vertrauliche Informationen offenlegen oder falsche Informationen verteilen. Es ist auch möglich, dass ein Angreifer auf diesem Weg Schadsoftware einspielt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.5.3 *Allgemeiner E-Mail-Client und -Server* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer, Vorgesetzte

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* 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 Benutzern vorkonfiguriert übergeben werden.

Die Institution MUSS sicherstellen, dass sicherheitsrelevante Teile der Konfiguration nicht von Benutzern geändert werden können. Ist dies nicht möglich, MUSS die Institution die Benutzer darauf hinweisen, dass die Konfiguration nicht selbstständig geändert werden darf.

Bevor Dateianhänge aus E-Mails geöffnet werden, MÜSSEN sie auf dem Client von einem Schutzprogramm auf Schadsoftware überprüft werden, sofern dies nicht bereits auf dem E-Mail-Server geschieht. 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 unkontrollierte, 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)

Der IT-Betrieb MUSS Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergreifen. Für den E-Mail-Empfang sowie den Zugriff von E-Mail-Clients über öffentliche Datennetze MÜSSEN E-Mail-Server eine sichere Transportverschlüsselung anbieten. Versenden E-Mails-Server von sich aus E-Mails, SOLLTEN sie dafür ebenfalls eine sichere Transportverschlüsselung nutzen.

Die Institution MUSS alle erlaubten E-Mail-Protokolle und Dienste festlegen. Außerdem MUSS der IT-Betrieb den E-Mail-Server so einstellen, dass er nicht als Spam-Relay missbraucht werden kann.

Werden Nachrichten auf einem E-Mail-Server gespeichert, MUSS der IT-Betrieb eine geeignete Größenbeschränkung für das serverseitige Postfach einrichten und dokumentieren.

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 MÜSSEN mit dem Datenschutzbeauftragten, der Personalvertretung und den Benutzern 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 den Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.5.3.A5 Festlegung von Vertretungsregelungen bei E-Mail-Nutzung [Vorgesetzte] (S)

Die Institution SOLLTE Vertretungsregelungen für die Bearbeitung von E-Mails festlegen. Werden E-Mails weitergeleitet, SOLLTEN die vertretenen Benutzer 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 Mitarbeiter die Autoreply-Funktionen nutzen, 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 Benutzer und Administratoren 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 Benutzer SOLLTE vorgeben,

- wie sich die Kommunikation absichern lässt,
- welche Benutzerzugriffsrechte es gibt,
- wie E-Mails auf gefälschte Absender 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 Mitarbeiter umgegangen werden soll,
- ob und wie Webmail-Dienste genutzt werden dürfen,
- wer für Gruppenpostfächer zuständig ist,
- wie mit Datei-Anhängen umgegangen werden soll und
- wie E-Mails im HTML-Format vom Benutzer behandelt werden sollen.

Die E-Mail-Sicherheitsrichtlinie SOLLTE ergänzend für Administratoren 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 Benutzer (S)

Die Institution SOLLTE die Benutzer darüber aufklären, welche Risiken beim Benutzen von E-Mail-Anwendungen bestehen und wie sie sicher mit E-Mails umgehen können. Dies SOLLTE zusätzlich zur allgemeinen Schulung und Sensibilisierung geschehen.

Die Institution SOLLTE die Benutzer über die Gefahren sensibilisieren, die entstehen können, wenn E-Mail-Anhänge geöffnet werden. Die Schulungen SOLLTEN ebenfalls darauf eingehen, wie Benutzer E-Mails von gefälschten Absendern erkennen 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 Benutzer [Benutzer] (S)

Grundsätzlich SOLLTEN Benutzer alle Spam-E-Mails ignorieren und löschen. Benutzer 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 Benutzer 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 überprüfen. Die Institution SOLLTE selbst DomainKeys und SPF einsetzen, um von ihr versendete E-Mails zu authentisieren.

Wird SPF verwendet, SOLLTE eindeutig vorgegeben werden, wie mit E-Mails verfahren werden soll. 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-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 den Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.5.3.A10 Ende-zu-Ende-Verschlüsselung (H)

Die Institution SOLLTE eine Ende-zu-Ende-Verschlüsselung sowie 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 mehrere redundante E-Mail-Server betreiben. Die redundanten E-Mail-Server SOLLTEN mit geeigneter Priorität in den DNS-Informationen 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 Blacklists (H)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, ob die E-Mail-Server der Institution auf öffentlichen Spam- oder Black-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 Infomation 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 Dokuemt "BSI TR-03108 Sicherer E-Mail-Transport" informationen darüber zur Verfügung, wie E-Mails sicher versendet werden können.

5. Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.45 Datenverlust

G 0.25 Ausfall von Geräten oder Systemen