Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Informationssicherheit auf Basis von ISO/IEC 27001
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 6.2
Version:	1.8

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: de-mail@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Modul der Technischen Richtlinie De-Mail beschreibt die Anforderungen für eine Zertifizierung des erforderlichen Managementsystems für Informationssicherheit (ISMS[1]) gemäß ISO/IEC 27001 zur Erlangung eines Testats Informationssicherheit nach De-Mail-Gesetz und bietet somit eine Alternative zur bisher zwingend erforderlichen ISMS-Zertifizierung nach IT-Grundschutz.

Basis für die Erlangung eines Testats Informationssicherheit nach De-Mail-Gesetz kann für den DMDA damit auch ein ISO/IEC 27001-Zertifikat sein. Mit diesem Zertifikat muss nachgewiesen werden, dass die in diesem Dokument definierten Anforderungen erfüllt, d. h. umgesetzt und auditiert sind.

Die De-Mail spezifischen Anforderungen aus den bereits existierenden TR-Modulen zum Thema Informationssicherheit wurden hier auf die Normenreihe der ISO/IEC 27000 abgebildet. Basis für das vorliegende Dokument waren die ISO/IEC 27001:2013 (im Folgenden mit [27001] bezeichnet) und die ISO/IEC 27002:2013 (im Folgenden mit [27002] bezeichnet).

Ein Abkürzungs- und Literaturverzeichnis ist im Dachdokument enthalten.

1 **I**nformation **S**ecurity **M**anagement **S**ystem

2 Aufbau des Dokuments

Das Kapitel 3 gibt Hinweise und definiert Anforderungen bei einem Vorgehen gemäß der [27001].

Rahmenbedingungen für die Auditierung in Form von Vorgaben für den Auditor, das eigentliche Audit und die Auditberichte sind in Kapitel 4 aufgeführt.

Die durch den DMDA umzusetzenden Anforderungen finden sich ab Kapitel 5. Dabei entspricht die Kapitelnummerierung der Systematik der [27002] und ermöglicht so eine direkte Integration in die individuelle Sicherheitskonzeption.

Zu den einzelnen Anforderungen der [27002] können folgende Zusätze definiert sein:

- De-Mail spezifische Umsetzungshinweise
  Bietet Hinweise auf De-Mail spezifische Belange. Damit werden keine neuen Anforderungen definiert sondern lediglich Informationen zur Umsetzung von Maßnahmen im Umfeld von De-Mail gegeben.
- De-Mail spezifische Ergänzung
  Bestehende Anforderungen der [27002] werden durch neue Anforderungen ergänzt. Diese erhalten eine eigene neue Kapitelnummer und sind durch bisher in der Technischen Richtlinie De-Mail formulierte Anforderungen definiert.

Die ergänzten Anforderungen aus der [27002] sind zur Übersicht im Anhang nochmals tabellarisch aufgeführt.

3 Vorgehensweise nach ISO

Dieses Kapitel beschreibt die Besonderheiten bei der Anwendung und Vorgehensweise gemäß der ISO/IEC 27000-Normen im De-Mail-Umfeld. Hierbei lassen sich grundsätzlich zwei Szenarien vorstellen:

1. Wird das ISMS gemäß [27001] erstmalig zertifiziert, werden die Anforderungen aus der ISO/IEC-Norm zusammen mit den De-Mail spezifischen Anforderungen während eines Audits geprüft.

2. Liegt bereits ein Zertifikat gemäß [27001] vor, sind in einem weiteren Audit die De-Mail-spezifischen Anforderungen zu prüfen und zu bestätigen.

In beiden Szenarien ist darauf zu achten, dass der Scope des ISMS die gesamte Infrastruktur umfasst, die den De-Mail-Betrieb beinhaltet. D. h. sämtliche für den De-Mail-Betrieb erforderliche IT, Räumlichkeiten, Personal sowie alle notwendigen Prozesse müssen im Scope des ISMS enthalten sein. Die Einhaltung dieser Anforderung ist durch den Auditor zu bestätigen (Auditbericht).

Wichtiger Aspekt bei beiden Vorgehensweisen ist die Ergänzung der Anforderungen der ISO/IEC-Norm durch De-Mail spezifische Anforderungen. Dazu werden die einzelnen Anforderungen ab Kapitel 5 mit dem Hinweis „De-Mail spezifische Ergänzung“ geeignet ergänzt.

Anforderungen aus der ISO/IEC-Norm, die Ergänzungen für De-Mail enthalten, sind im Anhang in einer separaten Tabelle (vgl. Tabelle A.2) zur Übersicht aufgeführt. Damit wird dem Auditor eine einfache Möglichkeit eröffnet, in einem bereits nach [27001] zertifizierten Bereich ergänzend die De-Mail-spezifischen Anforderung zu prüfen.

Bei der Vorgehensweise nach [27001] ist insbesondere darauf zu achten, dass eine Risikoakzeptanz nur in begründeten Ausnahmefällen ohne die Ergreifung von Maßnahmen erfolgen darf.

4 Anforderungen an die Auditierung

Das Kapitel beschreibt Besonderheiten bei der Auditierung, die sowohl den Auditor, das eigentliche Audit und den vom Auditor zu erstellenden Auditbericht betreffen.

4.1 Auditor

Die Auditoren müssen beim BSI für den Geltungsbereich De-Mail zertifiziert sein. Das Verfahren der Personenzertifizierung und die konkreten Anforderungen an die Auditoren sind beim BSI in den Dokumenten [VB_Personen] und [Prog_Personen] beschrieben.

4.2 Audit

Für den Abschluss der Testierung sind bei der erstmaligen Zertifizierung ein Penetrationstest und eine IS-Kurz-Revision durchzuführen und zu dokumentieren. Vorgaben hierfür finden sich in den Dokumenten [IS-Rev] und [PenTest].

4.3 Auditbericht

Der vom Auditor vorgelegte Auditbericht soll insbesondere dokumentieren, dass die in diesem Dokument aufgeführten De-Mail spezifischen Anforderungen beim DMDA geprüft und umgesetzt wurden. Hierzu wird eine Checkliste zur Verfügung gestellt.

5 Sicherheitsleitlinie

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 5 sind entsprechend anzuwenden.

Vgl. TR De-Mail:

[TR DM IS M] 3.1 Verfahren nach IT-Grundschutz

6 Organisation der Informationssicherheit

6.1 Interne Organisation

6.1.1 Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit

Die Maßnahme 6.1.1 der [27002] ist entsprechend anzuwenden.

Vgl. TR De-Mail:

- [TR DM IS M] 3.1 Verfahren nach IT-Grundschutz

6.1.2 Aufgabentrennung

Die Maßnahme 6.1.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Es muss ein Rollen- und Rechtekonzept entwickelt und dokumentiert werden, das den Grundsätzen der Funktionstrennung und nur den berechtigten Personen den Zugriff erlaubt.

Rollenausschlüsse ergeben sich dabei aus den folgenden grundsätzlichen Einschränkungen:

1. Keine Leitungsfunktion (wie Leiter DMDA, IT-SiBe, DSB) darf operative oder administrative Aufgaben übernehmen.
2. Keine Kontrollfunktion darf operative oder administrative Aufgaben übernehmen (Überwachung des Logging / Monitoring).
3. Die vollen Administrationsrechte müssen auf wenige Personen reduziert werden.
4. Rollen mit Zugriff auf gespeicherte Daten oder Daten, die übertragen werden, dürfen keinen Zugriff auf die verwendeten Schlüssel haben.
5. Der Zutritt zu Hardware und Netzwerkinfrastruktur darf in der gleichen Rolle abgebildet werden. Änderungen an der Hardware und der Netzinfrastruktur müssen im 4-Augen-Prinzip erfolgen und sind mittels Logging zu protokollieren.
6. Die Aktivitäten zur Identitätserfassung und -verwaltung müssen für ein De-Mail-Konto von verschiedenen Personen ausgeführt werden.

Für die Umsetzung des Rollenkonzepts und der Rollenausschlüsse bietet sich die folgende Aufteilung an:

- Leiter DMDA
  - ist der Gesamtverantwortliche für den Betrieb.
- IT-Sicherheitsbeauftragter (IT-SiBe)
  - übernimmt die Aufgaben im Sinne des Managers für Informationssicherheit nach ISO/IEC 27001
- Datenschutzbeauftragter (DSB)

- übernimmt die Aufgabe des Datenschutzbeauftragten für den Bereich De-Mail und damit insbesondere für die Erfüllung der Anforderungen aus dem [DSKritKat]

- Rechenzentrumsadministrator (RZ-Admin)
  - hat Zutritt zum Rechenzentrum und Zugriff auf die Hardwarekomponenten
  - ist zuständig für alle Hardwareaufgaben
  - begleitet andere Administratoren bei der Arbeit an Hardwarekomponenten
  - hat Zugriff auf die zum Betrieb und Wartung notwendigen Logdaten
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zugriff auf Schlüsselmaterial
- Log-Administrator
  - hat alleinigen Zugriff auf das Sicherheitslogging. In den Sicherheits-Logdaten werden alle wesentlichen Änderungen/Aktivitäten der Administratoren auf den Systemen festgehalten.
  - Die normalen Log-Daten der Systeme/Anwendungen, die zur Wartung und Betrieb genutzt werden, unterliegen nicht den Einschränkungen des Rollenkonzept.
  - überwacht die System und Aktivitäten der anderen Administratoren
  - ist alleinig dem Leiter der Organisation unterstellt
  - hat keinen Zutritt zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial
- Systemadministrator (Sys-Admin)
  - leistet halbautomatische Arbeiten zur Applikationssteuerung
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zutritt zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial
- Anwendungsadministrator (Appl-Admin)
  - betreut die Anwendungen (z. B. Webserver, E-Mailserver, usw.) und das Betriebssystem
  - führt Softwareupdates, Patches, Konfigurationsänderungen durch
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zutritt zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial
- Schlüsseladministrator (Key-Admin)
  - ist zuständig für die Verwaltung von allen Schlüsseln und Zertifikaten
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zutritt zum Rechenzentrum

- hat keinen Zugriff auf verschlüsselte Daten

- Netzwerkadministrator (Net-Admin)
  - hat Zugriff auf Netzwerk- und Firewallsysteme
  - konfiguriert Firewall, Netzwerkdienst (z. B. DNS, usw.) und ähnliches
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zugriff auf Schlüsselmaterial
- Storageadministrator (Storage-Admin)
  - zuständig für den Betrieb der Datenbanken bzw. anderer Speichersysteme
  - hat keinen Zugriff auf das Sicherheitslogging
  - hat keinen Zutritt zum Rechenzentrum
  - hat keinen Zugriff auf Schlüsselmaterial

Die wesentlichen Aktivitäten der Administratoren werden zuverlässig im Sicherheitslogging erfasst.

Die Rollen schließen einander aus. Das bedeutet, dass eine Person nicht gleichzeitig zwei dieser Rollen einnehmen darf.

Die Rollen des Leiters DMDA, der Datenschutzbeauftragte und des IT-SiBe sind organisatorische Rollen, die keine operative Tätigkeit ausüben.

Die anderen Rollen sind für den Betrieb der Technik zuständig. Es ist hier abhängig vom DMDA, welche Personen für einen korrekten Betrieb anwesend sein müssen, um einen korrekten und den Sicherheitsbestimmungen entsprechenden Betrieb zu gewährleisten. Damit ist gemeint, welche Rollen z. B. 24/7 verfügbar sein oder nur Rufbereitschaft gewährleisten müssen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.2 Rollenkonzept
- [TR DM IS GS] 6.1.2.4 Rollenausschlüsse
- [TR DM IS GS] 7.1.1 Rollenkonzept (Beispiele)

6.1.3 Kontakt zu Behörden

Die Maßnahme 6.1.3 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Gemäß De-Mail-Gesetz ist die zuständige Behörde das BSI. Dabei gilt die Zuständigkeit für die Akkreditierung der DMDA und für die Aufsicht über die akkreditierten DMDA. Ansprechpartner für erforderliche Änderungsmitteilungen im Rahmen der für die Akkreditierung notwendigen Testierungsverfahren ist das Referat D24.

Als Aufsichtsbehörde für den Bereich Datenschutz ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu nennen.

Abschließend wird auf Ziffer 16.1 „Management von Informationssicherheitsvorfällen und Verbesserungen“ hingewiesen.

6.1.4 Kontakt mit Interessengruppen

Die Maßnahme 6.1.4 der [27002] ist entsprechend anzuwenden.

6.1.5 Informationssicherheit im Projektmanagement

Die Maßnahme 6.1.5 der [27002] ist entsprechend anzuwenden.

6.2 Mobilgeräte und Telearbeit

6.2.1 Leitlinie zu Mobilgeräten

Die Maßnahme 6.2.1 der [27002] ist entsprechend anzuwenden.

6.2.2 Telearbeit

Die Maßnahme 6.2.2 der [27002] ist entsprechend anzuwenden.

6.2.3 Remote-Administration

De-Mail spezifische Ergänzung

Die Remote-Administration der IT-Systeme in den verschiedenen Sicherheitszonen und des Firewall-Systems selbst dürfen nur über einen gesicherten Weg erfolgen. Der Kanal, durch den die Administration der IT-Systeme und Applikationen erfolgt, muss durch starke Verschlüsselung und starke Authentisierung geschützt werden.

Sofern die Remote-Administration aus Räumen erfolgt, die zu der gleichen Liegenschaft wie das Rechenzentrum des jeweiligen De-Mail-Dienstes gehören, muss der administrative Remote-Zugriff auf die IT-Systeme mindestens durch ein sicheres Passwort geschützt sein.

Sofern die Remote-Administration aus einem – in Bezug auf das Rechenzentrum – externen Gebäude erfolgt, hat eine Zwei-Faktor-Authentisierung zu erfolgen. Für die Administration der Benutzerdaten von Remote besteht ein „hoher“ Schutzbedarf. Bei der Absicherung dieses Zugangs hat der DMDA diesem Rechnung zu tragen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.3.2 Anforderungen an die Remote-Administration der IT-Systeme

7 Personalsicherheit

7.1 Vor der Anstellung

7.1.1 Überprüfung

Die Maßnahme 7.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Nach De-Mail-Gesetz muss der DMDA bzw. das bei ihm beschäftigte Personal die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit und Fachkunde besitzen. In diesem Zusammenhang haben die betreffenden Mitarbeiter zum Nachweis ihrer Zuverlässigkeit ein Führungszeugnis gemäß §30 Absatz 5 BZRG bei der zuständigen Behörde vorzulegen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.3 Fachkunde und Zuverlässigkeit des Personals

7.1.2 Arbeitsvertragsklauseln

Die Maßnahme 7.1.2 der [27002] ist entsprechend anzuwenden.

7.2 Während der Anstellung

7.2.1 Verantwortung des Managements

Die Maßnahme 7.2.1 der [27002] ist entsprechend anzuwenden.

Vgl. auch 7.2.2

7.2.2 Sensibilisierung, Aus und Weiterbildung zur Informationssicherheit

Die Maßnahme 7.2.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Der DMDA muss die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit und Fachkunde besitzen. In diesem Zusammenhang ist von besonderer Bedeutung, dass die Mitarbeiter des DMDA vor Aufnahme der Tätigkeit ausreichend geschult werden. Die Schulung beinhaltet u. a. eine Einarbeitung/Einweisung in die auszuübende Tätigkeit und eine Sensibilisierung der Mitarbeiter hinsichtlich der Sicherheitsrelevanz ihrer Arbeit sowie der datenschutzrechtlichen Rahmenbedingungen. Die Mitarbeiter müssen vom für De-Mail verantwortlichen Vorgesetzten (beispielsweise Leiter des Bereichs De-Mail) im laufenden Betrieb auf ihre Fachkunde hin beurteilt werden. Ggf. müssen durch den Vorgesetzten Nachschulungen veranlasst werden.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.3 Fachkunde und Zuverlässigkeit des Personals

7.2.3 Disziplinarverfahren

Die Maßnahme 7.2.3 der [27002] ist entsprechend anzuwenden.

7.3 Beendigung und Wechsel der Anstellung

7.3.1 Zuständigkeiten bei Beendigung oder Wechsel der Anstellung

Die Maßnahme 7.3.1 der [27002] ist entsprechend anzuwenden.

8 Management von organisationseigenen Werten

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 8 sind entsprechend anzuwenden.

9 Zugriffskontrolle

9.1 Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle

9.1.1 Leitlinie zur Zugangskontrolle

Die Maßnahme 9.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Zugangskonzept

Zugang ist der Aufbau einer Verbindung zwischen einem IT-System und einem Nutzer, der ihm die Benutzung von Funktionen des IT-Systems ermöglicht.

Das Zugangskonzept muss festlegen, dass jedes IT-System des DMDA durch Mechanismen der Zugangskontrolle vor unberechtigtem Zugang geschützt sein muss. Es sind geeignete Mechanismen zur Authentisierung einzusetzen.

Der Zugang zu Systemen, auf denen unverschlüsselte Daten der Nutzer verarbeitet werden, muss strikt beschränkt und kontrolliert werden. Es sind Mechanismen vorzusehen, die das unbefugte Ausleiten von Daten unterbinden.

Zugriffskonzept

Zugriff ist der Vorgang, der einem Nutzer eines IT-Systems Informationen zugänglich macht, die als Daten in einem IT-System gespeichert sind. Dieser Vorgang kann beispielsweise lesend, schreibend oder ausführend erfolgen.
Das Zugriffskonzept muss die Realisierung des Zugriffschutzes auf schützenswerte Daten darlegen.

Das Zugriffskonzept ist so zu gestalten, dass Schlüsselinhaber keinen Zugriff auf IT-Systeme bekommen, auf denen die verschlüsselten Daten gespeichert werden.

Das Zugriffskonzept muss Mechanismen beschreiben, die sicherstellen, dass nur der berechtigte Benutzer Zugriff auf die für ihn gespeicherten Daten (z. B. De-Mails) erhält.

Des Weiteren müssen innerhalb des Zugriffskonzepts die Zugriffsberechtigungen auf den einzelnen Systemen im Sinne des Rollenkonzepts (siehe dazu auch Kapitel 6.1.2) festgelegt werden, d. h. der System-Administrator darf über volle Zugriffsrechte auf das entsprechende System verfügen. Für alle Anwendungen auf den IT-Systemen werden durch den System-Administrator separate Verzeichnisse angelegt und entsprechend des Rollenkonzepts die Zugriffsrechte für die weiteren Administratoren festgelegt.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.2 Rollenkonzept
- [TR DM IS GS] 6.1.2.2 Zugangskonzept
- [TR DM IS GS] 6.1.2.3 Zugriffskonzept

9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Die Maßnahme 9.1.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Das DMDA-Netzwerk muss in Sicherheitszonen eingeteilt werden. Das externe Netz ist vom internen Netz zu trennen und in bedarfsorientierte Netzbereichen aufzuteilen:

a) Daten-Netz

b) Internes Netz

c) Externes Netz

Für das Management der sicherheitskritischen Komponenten ist ein separates Management-Netz einzurichten. Das Management-Netz muss vor Zugriffen aus anderen Netzen geschützt sein. Aufgrund dieser Anforderung ergibt sich eine Netzarchitektur, die auf dem generischen Netzplan aus [TR DM IS GS] Kapitel 2.3 aufbaut und eine beispielhafte Architektur darstellt.

Nicht authentifizierte sowie direkte Verbindungsversuche auf interne Systeme sind zu blockieren.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.4.1 Sicherheitszonen
- [TR DM IS GS] 6.4.3 Kommunikationsverbindungen

9.2 Benutzerverwaltung

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 9.2 sind entsprechend anzuwenden.

9.3 Benutzerverantwortung

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 9.3 sind entsprechend anzuwenden.

9.4 Kontrolle des Zugangs zu Systemen und Anwendungen

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 9.4 sind entsprechend anzuwenden.

10 Kryptographie

10.1 Kryptographische Maßnahmen

10.1.1 Leitlinie zur Nutzung von kryptographischen Maßnahmen

Die Maßnahme 10.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Der DMDA muss ein Kryptokonzept unter Berücksichtigung der folgenden Anforderungen erstellen.

Allgemeines

Das Kryptokonzept muss die aktuell geltenden Standards hinsichtlich der verwendeten Techniken, Algorithmen und Schlüssellängen berücksichtigen. In [TR 03116-4] sind die zurzeit geltenden Standards aufgeführt. Es ist regelmäßig zu prüfen, ob die Sicherheitseigenschaften der verwendeten Verfahren weiterhin gegeben sind. Dazu kann auf den Algorithmenkatalog für qualifizierte elektronische Signaturen [TR 02102] zurückgegriffen werden, sowie [TR 03116-4].

Im Kryptokonzept ist weiter darzulegen, auf welche Weise bei Wechsel der Schlüssel die vorhandenen Datenbestände mit den neuen Schlüsseln verschlüsselt werden.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.8.1 Allgemeines

Transportverschlüsselung Nutzer – De-Mail-Dienst

Bei der Kommunikation zwischen dem Nutzer (oder De-Mail-Gateway) und dem De-Mail-Dienst können vertrauliche Daten ausgetauscht werden. Diese Daten müssen einerseits vor dem Einblick Dritter geschützt sein, andererseits muss die Authentizität und Integrität dieser Daten gesichert sein.

Die Kommunikationsverbindungen zwischen Nutzer und De-Mail-Dienst müssen verschlüsselt erfolgen.

Die Systeme des DMDA müssen sich gegenüber dem Nutzer authentisieren. Der DMDA muss dem Nutzer den/die Fingerprints des/der verwendeten Zertifikats/Zertifikate in geeigneter Weise zur Kenntnis bringen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.8.2 Transportverschlüsselung Nutzer – De-Mail-Dienst

Transportverschlüsselung DMDA-DMDA

Die Kommunikation von einem DMDA zu einem anderen muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen (TLS-Verbindung siehe [TR DM IT-BInfra IO]). Bei dem Kanalaufbau hat eine gegenseitige Authentisierung stattzufinden. Die verwendeten Zertifikate sind in einer Access Control List (ACL) zu hinterlegen.

Die Sperrlisten sind regelmäßig zu prüfen. Im Falle einer Revozierung eines SSL-Zertifikates muss dieses unverzüglich aus den ACLs entfernt werden.

Der DMDA hat Regelungen zur Kontrolle der kryptografischen Schlüssel für die gesicherte Verbindung im IT-Sicherheitskonzept zu treffen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.8.3 Transportverschlüsselung DMDA-DMDA

Transportverschlüsselung DMDA-intern

Die Kommunikation zwischen den Systemen des DMDA sollte verschlüsselt erfolgen. Es ist dabei nach Möglichkeit eine gegenseitige Authentisierung vorzusehen.

Vgl. TR De-Mail:

- [TR DMIS GS] 6.1.8.4 Transportverschlüsselung DMDA-intern

Schlüsselwechsel

Die verwendeten asymmetrischen Schlüssel für gespeicherte Inhalte und für die Transportverschlüsselung zwischen den DMDA sind nach drei Jahren auszutauschen.

Vgl. TR De-Mail:

- [TR DMIS GS] 6.1.8.5 Schlüsselwechsel

Einsatz der qualifizierten elektronischen Signatur

Es wird empfohlen, in die Zertifikate, die zur qualifizierten elektronischen Signatur eingesetzt werden, eine Einschränkung hinsichtlich ihres Verwendungszwecks zu integrieren. Eine mögliche Einschränkung kann z. B. lauten: „Nur zur Erfüllung von DMDA-Diensten“. Damit soll klargestellt werden, dass sich der DMDA den Inhalt der Nachricht nicht zueigen macht, sondern lediglich den Transport der Nachricht bestätigt.

Vgl. TR De-Mail:

- [TR DM IS GS] 7.1.3.1 Einsatz der qualifizierten elektronischen Signatur

Verwendung von Krypto-Hardware

Es wird empfohlen Krypto-Hardware (HSM) einzusetzen. Diese bietet den Vorteil, dass kein Zugriff auf den privaten Schlüssel erfolgen kann und somit ggf. der organisatorische Aufwand für die Verwaltung/Administration reduziert werden kann. Es sind jedoch Maßnahmen zu treffen, die die Verfügbarkeit der Dienste bei einem Defekt der Hardware sicherstellen. Dies ist im Sicherheitskonzept zu berücksichtigen.

Vgl. TR De-Mail:

- [TR DM IS GS] 7.1.3.2 Verwendung von Krypto-Hardware

10.1.2 Verwaltung kryptografischer Schlüssel

Die Maßnahme 10.1.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise
Bei der Schlüsselaufbewahrung muss gewährleistet werden, dass kein unbefugter Zugriff auf die Schlüssel erfolgen kann.

Bei der Verwendung von Softwareschlüsseln (Soft-PSE) z. B. für die TLS-Verbindung ist mit geeigneten Mitteln sicherzustellen, dass keine unberechtigten Kopien der Schlüssel erstellt werden können.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.8.6 Schlüsselaufbewahrung

11 Schutz vor physischem Zugang und Umwelteinflüssen

11.1 Sicherheitsbereiche

11.1.1 Physische Sicherheitszonen

Die Maßnahme 11.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail-spezifische Umsetzungshinweise

Gebäude

Die zum Betrieb von De-Mail erforderlichen technischen Einrichtungen müssen in einem Rechenzentrum untergebracht sein.

Die bauliche Anordnung und die Bausubstanz müssen den gängigen Richtlinien und Anordnung wie z. B. DIN, ISO, VDE, VDMA und Richtlinien des VdS entsprechen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.2.1 Gebäude

Sicherheitsbereiche im Rechenzentrum

Alle IT-Systeme, auf denen Klartextverarbeitung stattfinden, müssen in einem separaten Sicherheitsbereich im Rechenzentrum aufgestellt und betrieben werden. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Für die Administration der IT-Systeme und Anwendungen muss ein Sicherheitsbereich eingerichtet werden. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Das Datensicherungsarchiv muss in einem weiteren Brandabschnitt untergebracht sein und zutrittsgeschützt mit einer Zutrittskontrolltechnik versehen sein.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.2.2 De-Mail-spezifische Sicherheitsbereiche im Rechenzentrum

Zutrittskonzept
Der DMDA muss ein Zutrittskonzept erstellen. Die Anzahl der Zutrittsberechtigten muss dabei auf das notwendige Minimum beschränkt werden. Es ist sicherzustellen, dass sich in Räumen, in denen IT-Systeme mit vertraulichen Daten betrieben werden, niemals nur ein Mitarbeiter des DMDA allein aufhält (strikte Einhaltung des Vier-Augen-Prinzips).

Zutrittsschutz
IT- und Infrastrukturräume sind gegen unberechtigten Zutritt zu schützen. Dabei ist durch geeignete bauliche Maßnahmen oder auch die Verwendung anderer materieller Sicherungstechnik sicherzustellen, dass ein Zutritt Unbefugter hinreichend sicher ausgeschlossen werden kann.

In Bezug auf externe Täter bedeutet dies, dass die eingesetzte Infrastruktur einen so hohen Widerstandswert haben muss, dass der Versuch des unbefugten Zutritts mindestens so lange abgewehrt wird, wie es dauert, bis alarmierte Einsatzkräfte eintreffen.

Es ist mindestens eine Gefahrenmeldeanlage zu betreiben ist, die dem Stand von Wissenschaft und Technik entspricht. Auf Alarmmeldungen muss unverzüglich und angemessen reagiert werden können.

Es müssen hinreichende Zutrittskontrolltechniken zum Einsatz kommen.

Der Zutritt zu und der Aufenthalt in IT- und Infrastrukturräumen muss kontrolliert, überwacht und dokumentiert werden.

Für die Infrastruktur der Räume, in denen die Systeme für De-Mail betrieben werden, wird empfohlen, die nachfolgenden Mindestanforderungen umzusetzen. Dort, wo dies aufgrund baulicher Gegebenheiten nicht möglich erscheint, sollte untersucht werden, ob ggf. der Einsatz entsprechender Schutzschränke in Betracht kommt.

Für das Rechenzentrum sollte

- die Außenhaut mindestens Widerstandsklasse WK 5 (DIN V ENV 1627 bis 1630) aufweisen,
- die Türen und Fenster analog zur Außenhaut ausgestaltet sein.

Für den Sicherheitsbereich sollten

- die Wände mindestens Widerstandsklasse WK 3 (DIN V ENV 1627 bis 1630) aufweisen,
- die Türen analog zu den Wänden ausgestaltet sein.

Die Arbeitsumgebung der Administratoren muss räumlich so gestaltet sein, dass kein unbefugter Systemzugang und kein unbefugter Zugriff auf Systeme, Daten und Dokumente oder eine Kenntnisnahme vertraulicher Informationen möglich ist.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.2.1 Zutrittskonzept
- [TR DM IS GS] 6.2.3 Zutrittsschutz
- [TR DM IS GS] 7.2.1 Zutrittsschutz

11.1.2 Physische Zugangskontrollen

Die Maßnahme 11.1.2 der [27002] ist entsprechend anzuwenden.

11.1.3 Sicherung von Büros, sonstigen Räumen und Einrichtungen

Die Maßnahme 11.1.3 der [27002] ist entsprechend anzuwenden.

11.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Die Maßnahme 11.1.4 der [27002] ist entsprechend anzuwenden.

11.1.5 Arbeit in Sicherheitsbereichen

Die Maßnahme 11.1.5 der [27002] ist entsprechend anzuwenden.

11.1.6 Anlieferungs- und Ladezonen

Die Maßnahme 11.1.6 der [27002] ist entsprechend anzuwenden.

11.2 Sicherheit von Betriebsmitteln

11.2.1 Platzierung und Schutz von Betriebsmitteln

Die Maßnahme 11.2.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Es müssen hinreichende Zutrittskontrolltechniken zum Einsatz kommen.

Der Zutritt zu und der Aufenthalt in IT- und Infrastrukturräumen muss kontrolliert, überwacht und dokumentiert werden.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.2.3 Zutrittsschutz

11.2.2 Versorgungseinrichtungen

Die Maßnahme 11.2.2 der [27002] ist entsprechend anzuwenden.

11.2.3 Sicherheit der Verkablung

Die Maßnahme 11.2.3 der [27002] ist entsprechend anzuwenden.

11.2.4 Instandhaltung von Betriebsmitteln

Die Maßnahme 11.2.4 der [27002] ist entsprechend anzuwenden.

11.2.5 Entfernung von Werten

Die Maßnahme 11.2.5 der [27002] ist entsprechend anzuwenden.

11.2.6 Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude

Die Maßnahme 11.2.6 der [27002] ist entsprechend anzuwenden.

11.2.7 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln

Die Maßnahme 11.2.7 der [27002] ist entsprechend anzuwenden.

11.2.8 Unbeaufsichtigte Endgeräte

Die Maßnahme 11.2.8 der [27002] ist entsprechend anzuwenden.

11.2.9 Der Grundsatz des aufgeräumten Schreibtischs des leeren Bildschirms

Die Maßnahme 11.2.9 der [27002] ist entsprechend anzuwenden.

12 Betriebssicherheit

12.1 Betriebsverfahren und Zuständigkeiten

12.1.1 Dokumentierte Betriebsverfahren

Die Maßnahme 12.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Die Prozesse im Umgang mit den IT-Systemen des DMDA (Installation, Konfiguration, Administration) sind zu dokumentieren und nachzuweisen. Entsprechend der Dokumentation hat die sichere Installation, Konfiguration und Administration der eingesetzten IT-Systeme zu erfolgen. Die für die Mitarbeiter verfügbaren Dokumente zur Durchführung von Prozessen, Checklisten und Verfahrensanweisungen, sowie Handbücher sind in Zusammenarbeit mit den Mitarbeitern und insbes. des IT-Sicherheitsbeauftragten zu erstellen. Die Dokumentation muss möglichst einfach nachzuvollziehen zu sein.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.9 Dokumentation der Administrationsprozesse

Für jedes sicherheitskritische IT-System für De-Mail ist ein Betriebshandbuch zu führen. Dieses muss die aktuelle Konfiguration und Parametrisierung des Betriebssystems, der Dienste und der darauf installierten Applikationen enthalten. Änderungen an der Konfiguration sind zu vermerken und zu begründen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.3.7 Betriebshandbücher

12.1.2 Änderungsmanagement

Die Maßnahme 12.1.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Auf allen Systemen des DMDA darf nur freigegebene Software installiert werden. Gleiches gilt für die einzusetzende Hardware. Die Freigabe erfolgt durch den IT-Sicherheitsbeauftragten nach definierten Kriterien und nach erfolgreicher Durchführung von Tests, soweit diese erforderlich sind.

Der IT-Sicherheitsbeauftragte ist in den Changemanagementprozess einzubinden. Der IT-Sicherheitsbeauftragte überwacht die zugriffsgeschützte Lagerung der Original-Datenträger der eingesetzten Software. Hardware, die vor dem Einsatz beim DMDA bereits genutzt wurde, muss vor dem Einsatz von beeinflussenden Restdaten befreit werden.

Es ist sicherzustellen, dass alle relevanten Sicherheitspatches installiert werden. Vor der Installation sind die im Rahmen des Changemanagements entwickelten Regeln zu beachten.

Änderungen müssen an die Zertifizierungsstelle gemeldet werden.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.4 Changemanagement

- [TR DM IS GS] 6.3.3 Aktualität der Software
- [TR DM IS GS] 7.1.2 Empfehlungen zum Changemanagement

12.1.3 Kapazitätsmanagement

Die Maßnahme 12.1.3 der [27002] ist entsprechend anzuwenden.

12.1.4 Trennung von Entwicklungs, Test und Betriebsumgebungen

Die Maßnahme 12.1.4 der [27002] ist entsprechend anzuwenden.

12.2 Schutz vor Malware

12.2.1 Kontrollmaßnahmen gegen Malware

Die Maßnahme 12.2.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Alle IT-Systeme sind mit geeigneten Mitteln gegen Angriffe mit Schadsoftware zu schützen. Es ist sicherzustellen, dass Infektionen mit Schadprogrammen zuverlässig erkannt und die Schadsoftware unverzüglich beseitigt wird.

Durch geeignete Maßnahmen ist sicherzustellen, dass Nachrichtenentwürfe, die vom Absender dem Postfach- und Versanddienst übergeben werden, unmittelbar nach Übermittlung auf Schadsoftware geprüft werden.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.3.5 Schadsoftwareschutz
- [TR DM PVD Si] 5.1 Prüfung auf Schadsoftware

12.3 Backup

12.3.1 Datensicherungen

Die Maßnahme 12.3.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Der DMDA hat zur Sicherung von Informationen ein Konzept zu erarbeiten, das die Sicherung von sämtlichen relevanten Daten festlegt. Die Wiederherstellung von Daten, die durch den berechtigten Nutzer gelöscht wurden, ist nicht verpflichtend.

Die Datensicherung muss folgende Anforderungen erfüllen:

- Es darf nicht zu Datenverlust von Nutzerdaten kommen.
- Soweit die Daten im Speicher verschlüsselt vorliegen, sind diese auch verschlüsselt in die Datensicherung zu übernehmen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.7 Datensicherungskonzept
- [TR DM DA Si] 5.2 Backup-Konzept

12.3.2 Archivierungskonzept

De-Mail spezifische Ergänzung

Der DMDA hat ein Archivierungskonzept zu erstellen, in dem insbesondere die dauerhafte Archivierung von Protokollen und anderen Betriebsdaten, die durch einen De-Mail-Dienst entstehen, berücksichtigt werden muss.
Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.1 Archivierungskonzept

12.4 Protokollierung und Überwachung

12.4.1 Ereignisprotokollierung

Die Maßnahme 12.4.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Sicherheits-Logdaten:

Alle sicherheitskritischen IT-Systeme müssen für den administrativen Zugriff und für Änderungen an der Konfiguration eine Protokollierungskomponente enthalten, die in der Lage ist, jedes der folgenden Ereignisse revisionsfähig zu protokollieren:

- Anmeldevorgänge am System (erfolgreiche und nicht erfolgreiche),
- versuchter Zugriff auf eine der Rechteverwaltung unterliegende Komponente,
- alle Administrations-Verbindungsversuche.

Bei nicht erlaubten Verbindungsversuchen muss eine fest definierte Alarmmeldung ausgegeben werden.

Um unbefugtes teilweises oder komplettes Löschen von Daten zu verhindern und um entsprechende Nachweise zu führen, ist sicherzustellen, dass entsprechende Zugriffe durch das mit der Administration betraute Personal zuverlässig protokolliert werden.

Betriebs-Logdaten:

Alle für den Betrieb und die Wartung relevanten Daten sollten erfasst werden, um beispielsweise auf Hardwareausfälle, Überlast-Situationen oder Fehler in der Anwendung geeignet reagieren zu können.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.3.8 Protokollierung

12.4.2 Schutz von Protokollinformationen

Die Maßnahme 12.4.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Um unbefugtes teilweises oder komplettes Löschen von Sicherheis-Logdaten zu verhindern und um entsprechende Nachweise zu führen, ist sicherzustellen, dass entsprechende Zugriffe durch das mit der Administration betraute Personal zuverlässig protokolliert werden.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.3.8 Protokollierung

12.4.3 Administrator- und Betreiberprotokoll

Die Maßnahme 12.4.3 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Die Prozesse im Umgang mit den IT-Systemen des DMDA (Installation, Konfiguration, Administration) sind zu dokumentieren und nachzuweisen. Entsprechend der Dokumentation hat die sichere Installation, Konfiguration und Administration der eingesetzten IT-Systeme zu erfolgen. Die für die Mitarbeiter verfügbaren Dokumente zur Durchführung von Prozessen, Checklisten und Verfahrensanweisungen, sowie Handbücher sind in Zusammenarbeit mit den Mitarbeitern und insbes. des IT-Sicherheitsbeauftragten zu erstellen. Die Dokumentation muss möglichst einfach nachzuvollziehen zu sein.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.9 Dokumentation der Administrationsprozesse

12.4.4 Zeitsynchronisation

Die Maßnahme 12.4.4 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Zeitquelle für den Zeitservice ist die gesetzliche Zeit (MEZ/MESZ), die von der Physikalisch-Technischen Bundesanstalt (PTB) als UTC (PTB) + 1 (2) realisiert und verbreitet (DFC77, Telefonzeitdienst der PTB, NTP) wird.

Folgende Anforderungen werden an den Zeitservice bei De-Mail gestellt:

- Die Uhrzeiten aller im De-Mail-System eingesetzten Komponenten sind über einen dedizierten Zeitserver, der über die oben geforderte gesetzliche Zeit verfügt, zu synchronisieren.
- Die Synchronisierung muss über gesicherte Kanäle erfolgen.
- Die Zeit wird über das separate Management-Netz verbreitet. Das Management-Netz dient unabhängig vom Netz der Nutzdaten der Administration der Systeme. Die Administration darf nur über dieses Netz möglich sein.
- Die Zeitinformation, die der Zeitserver zur Verfügung stellt, darf max. 1 Sekunde von der gesetzlichen Zeit abweichen.
- Durch geeignete technische Maßnahmen ist sicherzustellen, dass die Zeit des Zeitservers nicht manipuliert werden kann. Es ist auch sicherzustellen, dass Manipulationen am Zeitsignal sicher erkannt werden. Dies kann beispielsweise durch den Abgleich mit der Systemzeit eines Referenzsystems erfolgen.

- Die Betriebssysteme und die Anwendungssoftware der IT-Systeme, die den Zeitservice für die jeweilige De-Mail-Infrastruktur zur Verfügung stellen, sind durch den Administrator regelmäßig, mindestens einmal täglich, auf Integrität zu überprüfen.

Vgl. TR De-Mail:

- [TR DM BInfra Si] 5.1.1 Zeitservice

12.5 Kontrolle von Betriebssoftware

12.5.1 Installation von Software auf betrieblichen Systemen

Die Maßnahme 12.5.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Die eingesetzten IT-Systeme sind sicher zu installieren und zu betreiben. Dabei sind insbesondere die Hinweise des jeweiligen Herstellers zu berücksichtigen.

Soweit zertifizierte IT-Systeme zum Einsatz kommen, sind die Auflagen hinsichtlich der Anforderungen an die Einsatzumgebung einzuhalten.

Alle IT-Systeme sind auf der Grundlage gehärteter Betriebssysteme zu installieren und zu betreiben. Hinsichtlich der verwendeten Betriebssysteme bedeutet dies, dass diese minimal zu installieren sind. Insbesondere sind alle nicht benötigten Dienste zu deaktivieren. Sie sind zudem zu deinstallieren, sofern dies das jeweilige Betriebssystem zulässt. Alle nicht benötigte Software darf nicht installiert werden bzw. ist zuverlässig zu deinstallieren.

Vor Inbetriebnahme sind die Systeme ausgiebig auf Funktionalität zu testen. Ein besonderer Fokus muss dabei auf den Sicherheitsfunktionen liegen. Hierzu ist ein gesondertes Testkonzept zu erstellen. Die Ergebnisse der Tests sind nachvollziehbar zu dokumentieren. Dies gilt entsprechend nach der Installation von Patches und Updates.

Es gilt der Grundsatz der minimalen Rechtevergabe für Benutzer; d. h. es dürfen nur die für die Aufgabenerfüllung absolut notwendigen Rechte vergeben werden. Die Rechtevergabe ist zu dokumentieren und zu begründen.

Durch geeignete Maßnahmen (beispielsweise Einstellung im BIOS) ist zu erzwingen, dass ein Systemstart nur vom Standard-Laufwerk aus erfolgt.

Das Betriebssystem oder die jeweilige Applikation müssen so konfiguriert werden, dass die im Rahmen des IT-Sicherheitskonzepts festgelegten Authentisierungsmechanismen genutzt werden müssen.

Durch geeignete technische Maßnahmen ist sicherzustellen, dass die Anmeldung eines Berechtigten an einem für De-Mail betriebenen IT-Systems nicht durch einen Unbefugten missbraucht werden kann. Daher ist sicherzustellen, dass, sofern der angemeldete Berechtigte seinen Arbeitsplatz auch nur kurzfristig verlässt, das betroffene IT-System für weitere Zugriffe gesperrt wird. Die Sperre darf nur aufgehoben werden, wenn eine erneute Authentisierung gegenüber dem IT-System erfolgt.

Vgl. TR De-Mail

- [TR DM IS GS] 6.3.4 Sichere Installation und sicherer Betrieb der eingesetzten IT-Systeme

12.5.2 Integritätsschutz für IT-Systeme

De-Mail spezifische Ergänzung

Alle für De-Mail betriebenen sicherheitskritischen IT-Systeme sind regelmäßig, mindestens einmal wöchentlich, mit geeigneten technischen Maßnahmen auf Integrität zu prüfen. Die Prüfung und das Ergebnis sind zuverlässig zu dokumentieren.

Sofern bei einer solchen Prüfung festgestellt wird, dass die Integrität des Systems verletzt wurde, sind unverzüglich geeignete Gegenmaßnahmen zu ergreifen. Hierzu ist präventiv ein entsprechender Ablaufplan, beispielsweise in Form einer Checkliste, zu erstellen.

Vgl. TR De-Mail

- [TR DM IS GS] 6.3.6 Integritätsschutz für IT-Systeme

12.6 Technisches Schwachstellenmanagement

12.6.1 Management technischer Schwachstellen

Die Maßnahme 12.6.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise
Es ist sicherzustellen, dass alle relevanten Sicherheitspatches installiert werden. Vor der Installation sind die im Rahmen des Changemanagements entwickelten Regeln zu beachten.

Sofern sicherheitszertifizierte IT-Systeme zum Einsatz kommen gilt folgendes:

- Sofern ein relevanter Patch bereits Gegenstand einer Re-Evaluierung war, so hat auch hier nach erfolgtem Freigabeverfahren die unverzügliche Installation zu erfolgen.
- Sofern ein Sicherheitspatch noch nicht Gegenstand der Re-Evaluierung war, ist durch das IT-Management zu entscheiden, wie zu verfahren ist. Dabei sind die möglichen Risiken gegeneinander abzuwägen. Das Ergebnis dieser Abwägung ist zu dokumentieren und umzusetzen.

Vgl. TR De-Mail

- [TR DM IS GS] 6.3.3 Aktualität der Software

12.6.2 Beschränkungen der Software-Installation

Die Maßnahme 12.6.2 der [27002] ist entsprechend anzuwenden.

12.7 Auswirkungen von Audits auf Informationssysteme

12.7.1 Kontrollen für Audits von Informationssystemen

Die Maßnahme 12.7.1 der [27002] ist entsprechend anzuwenden.

12.8 Web-Applikationen

12.8.1 Schutz der Web-Applikation

De-Mail spezifische Ergänzung

Die Web-Applikation ist durch geeignete Maßnahmen gegen unbefugte Zugriffe aus dem Internet und dem Intranet zu schützen. Zudem ist den aktuell bekannten Angriffen auf Web-Applikationen (z. B. SQL-Injection, Shell-Injection, Cross-Site-Scripting) durch geeignete Maßnahmen zu begegnen.

Es müssen alle Ein- und Ausgaben durch die Web-Applikation validiert werden. So muss vermieden werden, dass Metazeichen zu den Subsystemen weitergeleitet werden.

Zudem dürfen von der Web-Applikation keine detaillierten, systemspezifischen Fehlermeldungen an den Nutzer-Client weitergegeben werden. Interne Zustandsinformationen sollen ebenfalls an den Nutzer nicht übermittelt werden.

Zudem ist durch geeignete Maßnahmen sicherzustellen, dass durch Nutzer nur auf die öffentlichen Verzeichnisse des Webservers zugegriffen werden kann.

Ein Angreifer soll zudem keine Informationen über den verwendeten Webserver bekommen. Daher ist die Webserver-Identifizierung abzuschalten.

Die vom BSI herausgegebenen Best Practices [WebAppSec] sind zu berücksichtigen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.5.1 Schutz der Web-Applikation

12.8.2 Web-Applikations-Firewall

De-Mail spezifische Ergänzung

Die Web-Applikation selbst ist durch eine hoch stabile Sicherheitskomponente für die Web-Applikationssicherheit, die in den gesamten Datenverkehr zwischen den Nutzern und der Web-Applikation eingefügt wird, zu schützen. Dabei wird der gesamte Datenverkehr überwacht.

Die Web-Applikations-Firewall gewährleistet einen zusätzlichen Schutz auf Web-Applikationsebene. Damit entsteht hinter der Firewall ein zusätzlicher Sicherheitsbereich. Sämtliche Datenverbindungen in Richtung Portal- oder Web-Applikation werden in dieser Sicherheitsschleuse unterbrochen. Zugelassene Verbindungen werden permanent auf spezifische Datenstrukturen hin untersucht. Werden Angriffe erkannt, so erfolgt eine unmittelbare Unterbrechung der bestehenden Verbindung. Dies ist zu protokollieren.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.5.2 Web-Applikations-Firewall

12.9 Datenbanksicherheit

De-Mail spezifische Ergänzung

Für den Datenbankserver gelten insbesondere folgende Mindestanforderungen:

- Der Datenbank-Server muss im Datenbank-Netz des DMDA installiert werden.
- Die Kommunikationsverbindungen zum Datenbank-Server müssen durch die Firewall, insbesondere durch ein Application-Level-Gateway entsprechend abgesichert werden.
- Die Administration des Datenbankrechners, des Datenbanksystems und die Pflege der Daten in der Datenbank dürfen nur über das Management-Netz erfolgen.
- Auf der Ebene der Datenbank sind nur die unabdingbar notwendigen Berechtigungen einzurichten.
- Zugriffe aus anderen Datenbanken auf die betrachtete Datenbank sind wirksam zu unterbinden.
- Die Datenbankanwendung muss über geeignete Mechanismen eine sichere Identifikation und Authentisierung der Benutzer ermöglichen.
- Der unbefugte Zugriff auf vertrauliche Daten ist wirksam zu unterbinden.
- Die Datenbank-Anwendung muss eine Rollentrennung zwischen Administrator und Revisor unterstützen. Der Revisor darf als Einziger über die Berechtigung verfügen, die Protokolldateien auszuwerten und zu löschen.
- Zum Schutz der Datenbankintegrität muss die Datenbank-Software über ein vollständiges Transaktionssystem verfügen, welches dem ACID-Prinzip genügt.
- Die Datenbank ist in das Datensicherungskonzept mit einzubeziehen.

Die Regelungen für die Überwachungs- und Kontrollmechanismen sind explizit im IT-Sicherheitskonzept festzulegen.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.6.1 Anforderungen an die Datenbank

12.10 Öffentlicher Verzeichnisdienst (ÖVD)

De-Mail spezifische Ergänzung

Es darf ausschließlich der Applikationsserver Schreibrechte auf den ÖVD haben.

Alle Schreibzugriffe auf den ÖVD werden protokolliert. Bei Schreibzugriffen, die nicht durch den Server erfolgen, muss eine Alarmierung durch das Protokollierungssystem erfolgen.

Alle Berechtigungsänderungen auf dem ÖVD werden protokolliert. Bei Änderungen muss eine Alarmierung durch das Protokollierungssystem erfolgen.

Die Betriebssysteme und die Anwendungssoftware der IT-Systeme, die den öffentlichen Verzeichnisdienst für den jeweiligen De-Mail-Dienst zur Verfügung stellen, sind durch den Administrator regelmäßig, mindestens einmal täglich, auf Integrität zu überprüfen.

Es dürfen ausschließlich authentisierte De-Mail-Nutzer eine Verzeichnisdienstanfrage durchführen können.

Vgl. TR De-Mail:

- [TR DM BInfra Si] 5.1.2 ÖVD

12.11 Administration des DNS

De-Mail spezifische Ergänzung

Die Einträge im DNS-Server sind regelmäßig auf ihre Korrektheit zu prüfen. Es sollte DNSSEC zum Einsatz kommen.

Vgl. TR De-Mail:

- [TR DM BInfra Si] 5.2 Administration des DNS

13 Sicherheit in der Kommunikation

13.1 Netzwerksicherheitsmanagement

13.1.1 Netzwerkkontrollen

Die Maßnahme 13.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Die Trennung der Sicherheitszonen muss durch ein Firewall-System erfolgen. Das Firewall-System muss dem Stand von Wissenschaft und Technik entsprechen. Es muss aus einer Kombination von Paktetfiltern und Applikation-Level-Gateway bestehen.

Das Firewallsystem ist so sicher zu betreiben, dass unbefugte Zugriffe auf die dahinter liegenden IT-Systeme von außerhalb wirksam unterbunden werden.

Für das System ist ein Betriebshandbuch zu führen. Die Konfiguration sowie das Patchlevel sind zu dokumentieren. Änderungen an der Hard- und Software dürfen erst in Betrieb genommen werden, wenn zuvor die Funktionalität entsprechend getestet wurde.

Die anfallenden Protokolle sind regelmäßig, mindestens aber einmal täglich, zu überprüfen. Auf erkannte Angriffsversuche ist angemessen zu reagieren.

Die Wirksamkeit des Firewall-Systems ist regelmäßig durch Penetrationstests zu überprüfen.

Empfohlene Einzelanforderungen sind in [WebAppsec] zu finden.

Nicht authentifizierte sowie direkte Verbindungsversuche auf interne Systeme sind zu blockieren.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.4.2 Firewall-System (Sicherheitsgateway)
- [TR DM IS GS] 6.4.3 Kommunikationsverbindungen

Die eingesetzte Firewall-Technik muss im Hinblick auf den Aspekt Informationsflusskontrolle und korrekte Umsetzung eines Regelwerks zur Informationsflusskontrolle möglichst mindestens nach CC EAL 3 evaluiert und zertifiziert sein.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.1.10 Anforderungen an einzusetzende Hardware und Software

13.1.2 Sicherheit von Netzwerkdiensten

Die Maßnahme 13.1.2 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Der DMDA hat durch den Betrieb eines Intrusion Detection Systems (IDS), das dem Stand von Wissenschaft und Technik entspricht, sicherzustellen, dass Angriffe auf das De-Mail-Portal zuverlässig entdeckt werden. Es ist zudem durch geeignete organisatorische und technische Maßnahmen sicherzustellen, dass bei sicherheitskritischen Angriffen eine zuverlässige

unverzügliche Alarmierung erfolgt und unverzüglich angemessen auf einen solchen Angriff reagiert wird.

Vgl. TR De-Mail:

- [TR DM IS GS] 6.4.4 Intrusion Detection System

13.1.3 Trennung in Netzwerken

Die Maßnahme 13.1.3 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Die sicherheitskritischen IT-Systeme dürfen nur über ein separates Management-Netz administriert werden. Das Management-Netz muss vor Zugriffen aus anderen Netzen geschützt sein.

Ferner muss das DMDA-Netzwerk in Sicherheitszonen eingeteilt werden. Das externe Netz ist vom internen Netz zu trennen und in bedarfsorientierte Netzbereiche aufzuteilen:

- Daten-Netz
- Internes Netz
- Externes Netz

Vgl. TR De-Mail:

- [TR DM IS GS] 6.3.1 Einsatz eines Management Netzes
- [TR DM IS GS] 6.4.1 Sicherheitszonen

13.2 Informationsübertragung

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 13.2 sind entsprechend anzuwenden.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen für Informationssysteme

14.1.1 Analyse und Spezifikation von Sicherheitsanforderungen

Die Maßnahme 14.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Der Leitgedanke der De-Mail-Konzeption ist die Bereitstellung eines sicheren Kommunikationsraumes. Ein De-Mail-Dienst muss eine sichere Anmeldung, Nutzung eines PVD für sichere elektronische Post sowie die Nutzung eines ÖVD ermöglichen.
Innerhalb des Kommunikationsraumes sind insbesondere folgende Grundwerte zu gewährleisten:

- Verfügbarkeit
  - von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern jederzeit stets wie gewünscht (mit Ausnahme zumutbarer Ausfallzeiten) zur Verfügung stehen.
- Vertraulichkeit
  - ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich gemacht werden.
- Integrität
  - im engeren Sinne bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Informationen" wird dabei für Daten verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Bei De-Mail ist eine nutzenorientierte Datenhaltung zu realisieren. Eine strikte Trennung der Nutzer ist erforderlich, um zu verhindern, dass diese gegenseitigen Einblick in ihre Daten erhalten können.

Den Sicherheitsanker in De-Mail bildet das De-Mail-Konto. Ein De-Mail-Konto ist ein Bereich in einem De-mail-Dienst, der einem Nutzer so zugeordnet ist, dass er nur von ihm genutzt werden kann. Der DMDA hat durch technische Mittel sicherzustellen, dass nur der diesem De-Mail-Konto zugeordnete Nutzer Zugang zu dem ihm zugeordneten De-Mail-Konto erlangen

kann. Das De-Mail-Konto verwaltet die Zugangsberechtigung zum De-Mail-Dienst und damit die Berechtigung, die weiteren De-Mail-Dienste zu nutzen und auf Nutzerdaten zugreifen zu können. Sämtliches Handeln eines Nutzers ist unmittelbar mit dem De-Mail-Konto verbunden und lässt sich immer darauf zurückführen.

Um im De-Mail-Verbund handeln zu können, muss ein Nutzer sich am De-Mail-Dienst anmelden.

Übergreifende Aspekte

Daraus ergeben sich die im Folgenden beschriebenen übergreifenden Sicherheitsziele und Anforderungen. Diese Ziele gelten für De-Mail mit allen Diensten, die darin betrieben werden. Ergänzend sind die zu den einzelnen Diensten spezifisch definierten Anforderungen zu berücksichtigen.

Wahrung der Vertraulichkeit

Die Wahrung der Vertraulichkeit der gespeicherten und zu übertragenden Daten ist durch geeignete organisatorische und technische Maßnahmen sicherzustellen.

Dies beinhaltet insbesondere:

- Vermeidung unbefugten Zutritts,
- Verhinderung des unbefugten Zugangs,
- Verhinderung des unbefugten Zugriffs auf sensible Daten und
- verschlüsselte Speicherung und Transport der Daten.

Wahrung der Integrität

Durch geeignete Maßnahmen ist sicherzustellen, dass Daten nicht unbemerkt verändert werden können. Dies betrifft die Daten, die beim DMDA gespeichert sind und die Daten, die zwischen zwei DMDA übertragen werden. Sofern unbefugte Veränderungen erfolgen, müssen diese feststellbar sein. Die Konfiguration von Diensten und Systemen darf ebenfalls nicht unbefugt verändert werden.

Sicherstellung der Verfügbarkeit

Durch geeignete Maßnahmen ist sicherzustellen, dass eine Verfügbarkeit von 99,5 % pro Jahr gewährleistet wird. Ein Ausfall bis zu 24 Stunden, im Falle eines katastrophalen Ereignisses bis zu 72 Stunden ist hinnehmbar.

Bei längerfristigen geplanten Ausfallzeiten von mehr als drei Stunden sind die Nutzer rechtzeitig im voraus zu informieren.

Aufrechterhaltung des IT-Sicherheitsniveaus

Die Aufrechterhaltung des notwendigen IT-Sicherheitsniveaus ist durch den DMDA geeignet sicherzustellen. Zu diesem Zweck ist die Einhaltung und Fortschreibung des IT-Sicherheitskonzepts sicherzustellen.

Korrekte Authentisierung

Der DMDA muss sicherstellen, dass die Authentisierung der Nutzer gemäß den Anforderungen aus [TR DM ACM FU] zuverlässig und mit dem jeweils vorgegebenen Authentisierungsniveau erfolgt.

Anforderungen an einzusetzende Hard- und Software

Der eingesetzte Authentisierungsserver muss im Hinblick auf die korrekte Implementierung der Authentisierungsverfahren und der Kryptoalgorithmen dem aktuellen Stand der Technik entsprechen.

Der DMDA muss sich in geeigneter Weise von der Korrektheit der Implementierung der o.g. Verfahren und Algorithmen überzeugen.

Der CSP des DMDA muss im Hinblick auf die korrekte Implementierung der verwendeten Kryptoalgorithmen und den Zugriffsschutz auf geheime Schlüssel dem Stand von Wissenschaft und Technik entsprechen.

Vgl. TR De-Mail:

- [TR DM IS GS] 5.1 Vorbemerkungen
- [TR DM IS GS] 5.2 Übergreifende Aspekte
- [TR DM IS GS] 6.1.10 Anforderungen an einzusetzende Hardware und Software

14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzen

Die Maßnahme 14.1.2 der [27002] ist entsprechend anzuwenden.

14.1.3 Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten

Die Maßnahme 14.1.3 der [27002] ist entsprechend anzuwenden.

14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 14.2 sind entsprechend anzuwenden.

14.3 Prüfdaten

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 14.3 sind entsprechend anzuwenden.

15 Lieferantenbeziehungen

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 15 sind entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Sofern wesentliche Bereiche des IT-Verbunds (Infrastruktur, Personal) ausgelagert werden, sind weitere Anforderungen zu berücksichtigen.

Vgl. TR De-Mail:

- [TR DM M Si] 3.3.4 Modellierung

Anmerkung:

Hier sind insbesondere die Prozesse bei den Identifizierungsdienstleistern und die von diesen an die DMDA übertragenen Informationen (Ident-Daten) zu betrachten.

16 Management von Informationssicherheitsvorfällen

16.1 Management von Informationssicherheitsvorfällen und Verbesserungen

16.1.1 Zuständigkeiten und Verfahren

Die Maßnahme 16.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

In den festzulegenden Verfahren nach 16.1.1 Abschnitt b) ist der Kontakt zum BSI zu definieren. Es ist zu gewährleisten, dass entsprechende Meldungen an die nach De-Mail-Gesetz zuständige Behörde, das BSI, kommuniziert werden. Meldungen sind zu senden an

Bundesamt für Sicherheit in der Informationstechnik

Referat D24

Postfach 20 03 63

53133 Bonn

Mail-Adresse: referat-d24@bsi.bund.de oder referat-d24@bsi-bund.de-mail.de

16.1.2 Meldung von Informationssicherheitsereignissen

Die Maßnahme 16.1.2 der [27002] ist entsprechend anzuwenden.

16.1.3 Meldung von Informationssicherheitsschwachstellen

Die Maßnahme 16.1.3 der [27002] ist entsprechend anzuwenden.

16.1.4 Bewertung von und Entscheidung über Informationssicherheitsereignisse

Die Maßnahme 16.1.4 der [27002] ist entsprechend anzuwenden.

16.1.5 Reaktion auf Informationssicherheitsvorfälle

Die Maßnahme 16.1.5 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Informationssicherheitsvorfälle müssen an das BSI (Kontaktdaten siehe 16.1.1) gemeldet werden.

16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

Die Maßnahme 16.1.6 der [27002] ist entsprechend anzuwenden.

16.1.7 Sammeln von Beweismaterial

Die Maßnahme 16.1.7 der [27002] ist entsprechend anzuwenden.

17 Informationssicherheitsaspekte des Betriebskontinuitätsmanagements

17.1 Aufrechterhaltung der Informationssicherheit

Die Maßnahmenziele sowie die Inhalte der [27002] Kapitel 17.1 sind entsprechend anzuwenden.

17.2 Redundanzen

17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen

Die Maßnahme 17.2.1 der [27002] ist entsprechend anzuwenden.

17.2.2 Verfügbarkeitskonzept

De-Mail spezifische Ergänzung

Die Architektur und die De-Mail-Infrastruktur sind so auszulegen, dass die Vorgaben an die Verfügbarkeit erfüllt werden. Dazu muss der DMDA ein entsprechendes Verfügbarkeitskonzept erstellen. Das Verfügbarkeitskonzept muss Fehlerintoleranz und Fehlertoleranz berücksichtigen. Der DMDA muss darstellen, wie er durch geeignete Maßnahmen diese Anforderungen erfüllt.

Es ist ein Regelbetrieb von 7x24 Stunden mit hoher Verfügbarkeit vorzusehen. Durch geeignete Maßnahmen ist sicherzustellen, dass eine Verfügbarkeit von 99,5 % pro Jahr gewährleistet wird. Ein Ausfall bis zu 24 Stunden, im Falle eines katastrophalen Ereignisses bis zu 72 Stunden ist hinnehmbar.

Bei längerfristigen geplanten Ausfallzeiten von mehr als drei Stunden sind die Nutzer rechtzeitig im voraus zu informieren.

Vgl. TR De-Mail

- [TR DM Dachdokument] 7.5 Allgemeine Verfügbarkeit
- [TR DM IS GS] 5.2.3 Sicherstellung der Verfügbarkeit
- [TR DM IS GS] 6.1.5 Verfügbarkeitskonzept

17.3 Notfallkonzept

De-Mail spezifische Ergänzung

Es muss ein Notfallkonzept erstellt werden. Als Notfälle werden alle Ereignisse betrachtet, die die Verfügbarkeit der bestehenden materiellen und technischen Infrastruktur derart bedrohen, dass besondere Maßnahmen zur Sicherung oder Wiederaufnahme des Betriebs notwendig sind.

Das Notfallkonzept führt die Maßnahmen auf, die bei bestimmten Notsituationen durchzuführen sind, nennt weiterhin die entsprechenden Verantwortlichen und definiert die

einzuleitenden Schritte nach dem Notfall zur Wiedererlangung des Wirkbetriebs. Die „max. tolerierbare Ausfallzeit“ darf 24 Stunden, bei katastrophalen Ereignissen 72 Stunden nicht überschreiten.

Vgl. TR De-Mail

- [TR DM IS GS] 6.1.6 Notfallkonzept

18 Richtlinienkonformität

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

18.1.1 Feststellung anwendbarer Gesetze und vertraglicher Anforderungen

Die Maßnahme 18.1.1 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Insbesondere die Vorgaben aus dem De-Mail Gesetz und die Anforderungen der Technischen Richtlinie De-Mail sind zu berücksichtigen.

Ferner sind die vom BSI veröffentlichten Verfahrensbeschreibungen zu beachten, u. a. [VB_Produkte] und [VB_Akkr_De-Mail].

18.1.2 Rechte an geistigem Eigentum

Die Maßnahme 18.1.2 der [27002] ist entsprechend anzuwenden.

18.1.3 Schutz von Aufzeichnungen

Die Maßnahme 18.1.3 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Insbesondere die Vorgaben aus dem De-Mail Gesetz zu den Aufbewahrungspflichten sind zu beachten (vgl. § 13 De-Mail-Gesetz).

18.1.4 Privatsphäre und Schutz von personenbezogenen Informationen

Die Maßnahme 18.1.4 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Diese Anforderung wird durch das nach De-Mail-Gesetz geforderte Datenschutz-Zertifikat erfüllt (vgl. § 15 De-Mail-Gesetz).

18.1.5 Regulierung kryptographischer Kontrollmaßnahmen

Die Maßnahme 18.1.5 der [27002] ist entsprechend anzuwenden.

18.1.6 Identifizierung der Nutzer

De-Mail spezifische Ergänzung

Im Sicherheitskonzept des DMDA muss mindestens festgehalten werden:

- wie die Identitätsattribute erfasst werden,
- wie die Verifikation durchgeführt wird und
- wie die Übermittlung der Identitätsattribute sowie der Verifikationergebnisse erfolgt.

Bei der Übermittlung muss sichergestellt sein, dass:

– die Identitätsattribute korrekt sind und

– vertraulich übermittelt werden.

Sofern sich der DMDA zur Identifizierung der Nutzer vertrauenswürdiger Dritter bedient, hat er sicherzustellen, dass die Qualität des Gesamtprozesses einschließlich dessen Zuverlässigkeit und Fachkunde auch in diesem Fall gewährleistet wird.

Erfassung

Die Daten zur Identität sind zuverlässig im System zu hinterlegen und dem De-Mail-Konto zuzuordnen. Die Anbindung des Kontoadministrators an das Accountmanagement muss verschlüsselt, integer und authentisiert erfolgen. Für die Authentisierung sind Mechanismen wie bei dem Authentisierungsniveau „hoch“ einzusetzen.

Vgl. TR De-Mail

- [TR DM ACM Si] 5.1 Verifikation von Identitätsattributen
- [TR DM ACM Si] 5.2 Erfassung

18.1.7 Authentisierung der Nutzer

De-Mail spezifische Ergänzung

Authentisierungsniveaus

Für die Authentisierung des Nutzers sind folgende Authentisierungsmethoden für die beiden zugelassenen Authentisierungsniveaus vorzusehen:

- Normal

  Die Authentisierung erfolgt mittels Konto-Name und Passwort. Es sind insbesondere die einschlägigen Regeln zur Bildung und Gebrauch von Passwörtern zu beachten. Des Weiteren ist die maximale Gültigkeitsdauer für ein Passwort ein Jahr.

- Hoch

  Die Authentisierung muss mit zwei voneinander unabhängigen Sicherungsmitteln z. B. mit Besitz und Wissen erfolgen. Das Authentisierungstoken muss sicherstellen, dass das Geheimnis nicht kopiert und ausgelesen werden kann. Des Weiteren muss die Einmaligkeit der Authentisierungsinformationen, die innerhalb eines Anmeldeprozesses übertragen werden, gewährleistet sein. Die Authentisierung muss gleichen Anforderungen bei falscher Authentisierung und den Freischaltprozess erfüllen, wie das Authentisierungsniveau „normal“. Es sind die Anforderungen an die kryptographischen Verfahren und Schlüssellängen aus [TR 02102] zu beachten.

Authentisierung des Nutzers

Es ist sicherzustellen, dass der Nutzer keinen Zugriff auf sein De-Mail-Konto hat, bevor er sich ordnungsgemäß authentisiert hat. Der Nutzer hat sich jeweils vor Zugriff auf sein Konto gegenüber dem Dienst des DMDA mit Authentisierungsniveau „normal“ oder „hoch“ zu authentisieren.

Die Authentisierungsinformationen des Nutzers werden auf ihre Gültigkeit hin geprüft. Im Erfolgsfall wird der Nutzer zur Nutzung der gestatteten Funktionen autorisiert. Im Fehlerfall wird eine Fehlermeldung ausgegeben.

Der DMDA hat sich davon zu überzeugen, dass die bei der Erzeugung des Tokens für das Authentisierungsniveau „hoch“ eingesetzten Prozesse eine hinreichende Qualität und Vertrauenswürdigkeit in Bezug auf das angestrebte Authentisierungsniveau aufweisen. Wenn als Authentisierungstoken für das Authentisierungsniveau „hoch“ der nPA zum Einsatz kommt, darf der DMDA ohne weiteres von der Eignung des Tokens und der Ordnungsmäßigkeit der diesbezüglichen Prozesse ausgehen.

Vgl. TR De-Mail

- [TR DM ACM Si] 5.3 Authentisierungsniveaus
- [TR DM ACM Si] 5.4 Authentisierung des Nutzers

18.2 Informationssicherheitsprüfungen

18.2.1 Unabhängige Prüfung der Informationssicherheit

Die Maßnahme 18.2.1 der [27002] ist entsprechend anzuwenden.

18.2.2 Einhaltung von Sicherheitsleitlinien und -normen

Die Maßnahme 18.2.2 der [27002] ist entsprechend anzuwenden.

18.2.3 Technische Konformitätsprüfung

Die Maßnahme 18.2.3 der [27002] ist entsprechend anzuwenden.

De-Mail spezifische Umsetzungshinweise

Die IT-Systeme eines jeden De-Mail-Dienstes sind regelmäßigen, anlassbezogenen, mindestens aber jährlichen, Penetrationstests zu unterziehen. Sie sind nach folgendem Schema aufzubauen:

- Recherche nach Informationen über das Zielsystem,
- Scan der Zielsysteme auf angebotene Dienste,
- System- und Anwendungserkennung,
- Recherche nach Schwachstellen,
- Ausnutzen der Schwachstellen.

Vgl. TR De-Mail

- [TR DM IS GS] 6.3.9 Regelmäßige Penetrationstests

Anhang

In den Tabellen A.1 und A.2 werden die in den Kapiteln 5 bis 18 ergänzten, für De-Mail spezifischen Sicherheitskategorien, Maßnahmenziele und Maßnahmen, welche in der [27002] nicht aufgeführt sind, nochmals im Überblick dargestellt.

Tabelle A.1 — Überblick der ergänzten Sicherheitskategorien und Maßnahmenziele

Abschnitts-nummer	Titel	Maßnahmenziel	Seite
6.2.3	Remote-Administration	Gewährleistung der Informationssicherheit bei Nutzung von Remote-Administration	15
12.3.2	Archivierungskonzept	Langfristige Aufbewahrung betriebsrelevanter Informationen	30
12.5.2	Integritätsschutz für IT-Systeme	Sicherstellung der Integrität von betrieblichen IT-Systemen	33
12.8	Web-Applikationen	Schutz der Web-Applikationen	34
12.9	Datenbanksicherheit	Gewährleistung der Datenbank-Sicherheit	34
12.10	Öffentlicher Verzeichnisdienst (ÖVD)	Gewährleistung der Sicherheit des ÖVD	35
12.11	Administration des DNS	Sicherstellung der Korrektheit der DNS-Einträge	36
17.2	Redundanzen	Sicherstellung der Verfügbarkeit von informationsverarbeitenden Einrichtungen	45
17.3	Notfallkonzept	Aufrechterhaltung des De-Mail-Betriebs	45
18.1.6	Identifizierung der Nutzer	Die sichere Identifizierung des Kontoinhabers ist zu gewährleisten.	47
18.1.7	Authentisierung der Nutzer	Verhinderung eines unbefugten Zugriffs und einer unbefugten Veränderung von Authentisierungsinformationen.	48

Tabelle A.2 — Überblick der ergänzten Maßnahmen

Abschnitts-nummer	Titel	Maßnahme (stichwortartig)	Seite
6.2.3	Remote-Administration	Absicherung des Zugangs zur Remote-Administration	15
12.3.2	Archivierungskonzept	Archivierung der dauerhaft aufzubewahrenden Informationen	30
12.5.2	Integritätsschutz für IT-Systeme	Sicherheitskritische IT-Systeme sind regelmäßig, mindestens einmal wöchentlich, mit geeigneten technischen Maßnahmen auf Integrität zu prüfen	33
12.8.1	Schutz der Web-Applikationen	- Schutz vor unbefugtem Zugriff und vor bekannten Angriffen - Validierung der Ein- und Ausgaben - Einschränkung der protokollspezifischen Information - Berücksichtigung der Best Practices [WebAppSec]	34
12.8.2	Web-Applikation-Firewall	Nutzung einer entsprechenden Firewall	34
12.9	Datenbanksicherheit	Gewährleistung der Datenbank-Sicherheit durch verschiedene Maßnahmen	34
12.10	Öffentlicher Verzeichnisdienst (ÖVD)	Beschränkung und Prüfung der Zugriffsrechte auf den ÖVD	35
12.11	Administration des DNS	Regelmäßige Überprüfung der DNS-Einträge.	36
17.2.2	Verfügbarkeitskonzept	Es ist ein Verfügbarkeitskonzept zu erstellen. Ferner ist der 24/7 Regelbetrieb zu gewährleisten.	45
17.3	Notfallkonzept	Erstellung eines Notfallkonzepts	45
18.1.6	Identifizierung der Nutzer	Anforderungen an die Identifizierung und Ident-Dienstleister	47
18.1.7	Authentisierung der Nutzer	Sichere Authentisierung der Nutzer	48