Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Informationssicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 6
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

Dieses Modul beschreibt die Anforderungen zur Informationssicherheit an einen DMDA. Für den Nachweis der Erfüllung der Anforderungen stehen zwei Vorgehensweisen zur Verfügung: Der Nachweis kann entweder mittels eines ISO 27001-Zertifikats auf Basis von IT-Grundschutz oder alternativ mittels eines nativen ISO 27001-Zertifikats erfolgen, jeweils ergänzt um De-Mail-spezifische Anforderungen.

2 Aufbau des Moduls Informationssicherheit

2.1 Vorgehen nach IT-Grundschutz

Konzeptionelle Vorgaben für die Erstellung eines Sicherheitskonzeptes sind in folgenden Dokumenten enthalten. Die Dokumente enthalten die IT-Sicherheitsziele sowie daraus abgeleitet Maßnahmen, die zwingend umgesetzt werden müssen (Vorgaben) und solche, die durch alternative Maßnahmen ersetzt werden können (empfohlene Maßnahmen).

a) Technische Richtlinie De-Mail Informationssicherheit nach ISO 27001 auf Basis von IT-Grundschutz [TR DM IS GS]
Dieses Modul enthält eine beispielhafte, technische Abbildung einer De-Mail-Infrastruktur. Der in diesem Dokument skizzierte Ansatz kann dem DMDA als Beispiel für sein Sicherheitskonzept dienen. Die Anforderungen sind analog den Anforderungen für eine ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz keinesfalls vollständig und müssen an die jeweiligen individuellen Gegebenheiten angepasst werden.

Spezifische Sicherheitsaspekte einzelner De-Mail-Dienste werden in den nachfolgend benannten Modulen betrachtet:

b) Technische Richtlinie De-Mail Sicherheit Accountmanagement [TR DM ACM Si]
Es ist Bestandteil des Moduls Accountmanagement.

c) Technische Richtlinie De-Mail Sicherheit IT-Basisinfrastruktur [TR DM IT-BInfra Si]
Es ist Bestandteil des Moduls IT-Basisinfrastruktur.

d) Technische Richtlinie De-Mail Sicherheit – Postfach- und Versanddienst [TR DM PVD Si]
Es ist Bestandteil des Moduls Postfach- und Versanddienst.

e) Technische Richtlinie De-Mail Sicherheit – Dokumentenablage [TR DM DA Si]
Es ist Bestandteil des Moduls Dokumentenablage.

f) Technische Richtlinie De-Mail Sicherheit – Identitätsbestätigungsdienst [TR DM ID Si]
Es ist Bestandteil des Moduls Identitätsbestätigungsdienst.

Der Inhalt von a) bis d) ist in jedem Fall anzuwenden; hingegen ist eine Anwendung von e) bis f) nur notwendig, wenn der DMDA auch den jeweiligen Dienst tatsächlich anbietet.

2.2 Vorgehen nach ISO 27001

Das Dokument „Technische Richtlinie De-Mail Informationssicherheit auf Basis von ISO/IEC 27001“ [TR DM IS 27001] enthält sämtliche Anforderungen bei einer Vorgehensweise nach ISO/IEC 27001. Die Anforderungen sind dabei zum Teil als Erweiterungen zu den bestehenden Controls aus [27002] formuliert.

Optionale Anforderungen, die für die Dokumentenablage bzw. den Identitätsbestätigungsdienst relevant sind, sind entsprechend gekennzeichnet.

3 Ablauf der Verfahren

3.1 Verfahren nach IT-Grundschutz

Im Folgenden wird der Ablauf des Testierungsverfahrens auf der Basis von IT-Grundschutz unter besonderer Berücksichtigung der Anforderungen von De-Mail beschrieben.

3.1.1 Fokus

Grundlage für das durch den DMDA zu erstellende IT-Sicherheitskonzept sind folgende Standards: [BSI 100-1], [BSI 100-2] und [BSI 100-3] sowie [IT-GS-Kompendium]. Die darin enthaltenen Standard-Sicherheitsmaßnahmen decken bei vollständiger Umsetzung den normalen Schutzbedarf ab und stellen eine Basis für die adäquate Absicherung von höherem Schutzbedarf dar.

3.1.1.1 Definition des Informationsverbundes

In den Geltungsbereich fallen alle Dienste, die der DMDA im Rahmen dieses Projektes anbietet. Dazu ist durch den DMDA innerhalb des Sicherheitskonzepts der Untersuchungsgegenstand darzustellen und ggf. zu anderen von ihm angebotenen Diensten abzugrenzen.

3.1.1.2 Schutzbedarfsfeststellung

Angesichts der regelmäßig bei den De-Mail-Diensten verwendeten Daten ist grundsätzlich von einem hohen Schutzbedarf für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit auszugehen. Diese Festlegung entbindet nicht von der Prüfung, ob einzelne Systeme nicht einen sehr hohen Schutzbedarf ausweisen.

3.1.1.3 Modellierung

Im Rahmen der Modellierung eines Informationsverbunds „De-Mail“ sind nachfolgende Bausteine zwingend umzusetzen:

- B 1.0 IT-Sicherheitsmanagement
- B 1.3 Notfallvorsorgemanagement
- B 1.7 Kryptokonzept
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.12 Archivierung

Sofern wesentliche Bereiche des IT-Verbunds (Infrastruktur, Personal) ausgelagert werden, muss der De-Mail-Diensteanbieter folgenden IT-Grundschutzbaustein umsetzen:

- B 1.11 Outsourcing

Wichtig:

Im Rahmen der Modellierung sind über die Maßnahmen der jeweils zu betrachtenden Bausteine hinaus die Anforderungen aus den jeweiligen Modulen der Technische Richtlinie De-Mail [TR DM] zu berücksichtigen.

3.1.1.4 Penetrationstests und IS-Kurz-Revision

Das Prüfteam besteht aus vom BSI zertifizierten IS-Revisoren und Penetrationstestern oder aus Mitarbeitern des BSI.

Für den erfolgreichen Abschluss der in diesem Modul beschriebenen Testierung ist für jeden betroffenen De-Mail-Dienst ein IT-Penetrationstest sowie eine IS-Kurzrevision durchzuführen und zu dokumentieren. Dies dient der Vorabkontrolle der wesentlichen Sicherheitsmerkmale und der Feststellung grober Sicherheitsmängel. Dem DMDA soll damit die möglichst reibungslose Auditierung nach ISO 27001 auf Basis von IT-Grundschutz für De-Mail-Dienste erleichtert werden. Das diesbezügliche Vorgehen wird nachfolgend beschrieben.

Das IT-Penetrations-Testverfahren für De-Mail-Provider wird mehrstufig durchgeführt. Nach einem Web-Sicherheitsscheck ermittelt das Prüfteam auf Grundlage einer Dokumentenprüfung und einer Vor-Ort-Prüfung den Sicherheitsstatus des Providers. Betrachtet werden Prüfthemen, die eine wesentliche Grundlage für die Informationssicherheit bilden [PenTest].

Im ersten Schritt wird über das Internet die Webanwendung mittels verschiedener Tools auf Schwachstellen untersucht. Bei diesem Test geht es ausdrücklich um die Überprüfung der Sicherheitseigenschaften der Webanwendung und nicht um die Eigenschaften zusätzlich eingesetzter Sicherheitsgateways. Da Firewall-Regeln oft dynamisch im Betrieb verändert werden und alle Komponenten von Sicherheitsgateways ebenso, wie andere Systeme bei Schwachstellen ausgehebelt werden können, legt die Prüfung großen Wert darauf, dass bekannte Schwachstellen wie beispielsweise Cross-Site-Scripting oder Cross Site Request Forgery schon bei den Webanwendungen vermieden werden.

Um diese Tests durchführen zu können, ohne die Sicherheitsgateways abzuschalten, muss für das Prüfteam ein direkter Zugang zur Anwendung bestehen, der unmittelbar nach den Tests wieder entfernt werden kann. Wichtig ist, dass ein kompetenter Ansprechpartner des Providers vor Ort die Tests betreut und sie beobachtet.

Wenn der erste Web-Sicherheitscheck abgeschlossen ist, werden bei einem Vor-Ort Termin weitere Sicherheitseigenschaften getestet. Im Vorfeld der Vor-Ort-Prüfung wird die Dokumentation des Providers gesichtet, um eine Teststrategie zu entwickeln. Dazu erhält das Prüfteam Einsicht in die Dokumentation des Providers (z. B. Netzpläne, Liste der kritischen Geschäftsprozesse, IT-Sicherheitskonzept, Dokumentation der Anlage usw.). Zu Beginn der Vor-Ort-Prüfung findet ein Eröffnungsgespräch statt, in dem kurz die Vorgehensweise und die Zielrichtung der Prüfung und Tests erläutert werden. Bei der Vor-Ort-Prüfung werden Interviews geführt, die Liegenschaft begangen und die Systeme in Augenschein genommen. Das Prüfteam benötigt Shell-Zugänge zu den zu testenden Systemen, um die Konfigurationen zu überprüfen. Zur Analyse des Netzwerkverhaltens braucht das Prüfteam einen Mirror-Port an den zu testenden Stellen im Netzwerk oder die Möglichkeit, Taps anzuschließen, die bei Bedarf auch durch das Prüfteam gestellt werden können. Für Fragen zu den einzelnen Themen müssen kompetente Ansprechpartner verfügbar sein. Insbesondere sollte der IT-Sicherheitsbeauftragte das Prüfteam begleiten. Zusätzlich ist wichtig, dass ein Administrator des Providers die Tests direkt vor Ort betreut, damit Fragen geklärt werden können.

Zum Abschluss der Prüfungen und Tests wird eine Abschlussbesprechung durchgeführt. Hierbei werden die gefundenen Schwächen und Mängel präsentiert. Die Ergebnisse werden in einem Abschlussbericht zusammengefasst. Der De-Mail Provider muss bis zum Audit alle wesentlichen Mängel beseitigen und die Art und Weise der Beseitigung nachvollziehbar dokumentieren. Dieses Dokument ist dann dem zertifizierten De-Mail-Auditor zur Verfügung zu stellen.

3.1.2 Testat für den De-Mail IT-Verbund

Nach Umsetzung des IT-Sicherheitskonzeptes und Auditierung kann ein Testat auf Basis von IT-Grundschutz bei einem zertifizierten IT-Sicherheitsdienstleister beantragt werden, der das Testat ausstellt.

Für die Durchführung von Audits eines DMDA muss ein vom BSI zertifizierter De-Mail-Auditor gewählt werden.

Im Rahmen der Auditierung müssen dem zertifizierten De-Mail-Auditor und der Testatstelle dann folgende Referenzdokumente vom Antragsteller zur Verfügung gestellt werden:

- IT-Sicherheitsrichtlinien (A.0),
- IT-Strukturanalyse (A.1),
- Schutzbedarfsfeststellung (A.2),
- Modellierung des IT-Verbundes (A.3),
- Ergebnisse des Basis-Sicherheitschecks (A.4) (optionale Vorlage bei der Testatstelle; verpflichtende Vorlage beim zertifizierten De-Mail-Auditor),
- Ergänzende Sicherheitsanalyse (A.5),
- Risikoanalyse (A.6),
- Ergebnisse der IT-Penetrationstests,
- Ergebnisse der IS-Revision.

Einzelheiten zum Verfahren sind analog zur Zertifizierung in dem Dokument [Zert ISO 27001] festgelegt und anzuwenden.

3.2 Vorgehen nach ISO 27001 (nativ)

Im Folgenden wird der Ablauf des Testierungsverfahrens auf der Basis von ISO 27001 (nativ) unter besonderer Berücksichtigung der Anforderungen von De-Mail beschrieben.

3.2.1 Fokus

Grundlage für die durch den DMDA zu erstellende IT-Sicherheitskonzeption sind folgende Standards: [27001], [27002].

3.2.1.1 Definition des Informationsverbundes

In den Geltungsbereich fallen alle Dienste, die der DMDA im Rahmen dieses Projektes anbietet. Dazu ist durch den DMDA innerhalb der Sicherheitskonzeption der Untersuchungsgegenstand darzustellen und ggf. zu anderen von ihm angebotenen Diensten abzugrenzen.

3.2.1.2 Risikoakzeptanz

Angesichts der regelmäßig bei den De-Mail-Diensten verwendeten Daten ist grundsätzlich von hohen Anforderungen für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit auszugehen. Diese Festlegung entbindet nicht von der Prüfung, ob einzelne Systeme nicht sehr hohen Anforderungen unterliegen.

Eine Akzeptanz von Risiken ist nur begründeten Ausnahmen gestattet. Die gesetzlichen Anforderungen sind entsprechend zu berücksichtigen.

3.2.1.3 Penetrationstests und IS-Kurz-Revision

Die Anforderungen aus Kapitel 3.1.1.4 gelten hier ebenso und sind zu beachten bzw. umzusetzen.

3.2.2 Testat für den De-Mail IT-Verbund

Nach der Umsetzung der IT-Sicherheitskonzeption und Auditierung kann ein Testat bei einem zertifizierten IT-Sicherheitsdienstleister beantragt werden, der das Testat ausstellt. Als Grundlage für die Testierung kann ein ISO 27001-Zertifikat dienen, dass um die De-Mail-spezifischen Anforderungen ergänzt wurde bzw. diese bereits berücksichtigt.

Für die Durchführung von Audits eines DMDA muss ein vom BSI zertifizierter De-Mail-Auditor gewählt werden.

4 Ergänzende Anforderungen an den zertifizierten De-Mail-Auditor

Die für eine Auditierung von De-Mail-Diensten zu erfüllenden Voraussetzungen durch den zertifizierten De-Mail-Auditor ergeben sich aus der Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen [VB_Personen] sowie dem Programm zur Kompetenzfeststellung und Zertifizierung von Personen [Prog_Personen].

4.1 Vorgehensweise nach IT-Grundschutz

Hinsichtlich der Durchführung des Audits gelten grundsätzlich die Vorgaben von [Zert ISO 27001]. Der zertifizierte De-Mail-Auditor hat darüber hinaus insbesondere auch zu prüfen, ob die Festlegungen der Schutzbedarfsfeststellung in Übereinstimmung mit diesem Modul und [TR DM IS GS] erfolgt sind. Das Ergebnis dieser Prüfung ist gesondert darzustellen.

Zudem hat der zertifizierte De-Mail-Auditor zu überprüfen, ob bei der Durchführung der ergänzenden Sicherheitsanalyse und der Risikoanalyse die in den relevanten Teilen der Technischen Richtlinie De-Mail IT-Sicherheit festgelegten Sicherheitsziele und zwingenden Vorgaben beachtet und umgesetzt wurden. Das Ergebnis dieser Prüfungen ist explizit darzustellen.

4.2 Allgemein

In einigen der zwingenden Anforderungen der TR De-Mail ist daneben festgelegt, dass für die eingesetzten Produkte eine hinreichende Güte durch eine entsprechende Sicherheitszertifizierung nachgewiesen werden muss. Durch den zertifizierten De-Mail-Auditor ist daher zu prüfen, ob für die eingesetzten Produkte entsprechende Sicherheitszertifikate vorliegen und ob die Anforderungen an die Einsatzumgebung, die der Produktzertifizierung zugrunde liegen, eingehalten werden. Das Ergebnis dieser Prüfung ist darzustellen.

Für die Dokumentation der beschriebenen Zusatzprüfung wird dem zertifizierten De-Mail-Auditor ein Musterauditreport zur Verfügung gestellt, den der zertifizierte De-Mail-Auditor beim BSI anfordern kann.