Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	IT-Basisinfrastruktur IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 1.3
Version:	1.3

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 beinhaltet die IT-Sicherheitsanforderungen, die über die generellen Anforderungen aus dem Modul [TR DM Si M] hinausgehen und speziell für die IT-Basisinfrastruktur anzuwenden sind, und ist Bestandteil von [TR DM IT-BInfra M].

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die in [TR DM Si ÜK] angenommene Netzinfrastruktur eines DMDA.

Bei der Erstellung des realen IT-Sicherheitskonzepts sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der in [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Es werden in diesem Abschnitt nur die Bedrohungen für die IT-Basisinfrastruktur betrachtet, die sich zusätzlich zu den Bedrohungen aus [TR DM Si ÜK] durch die Funktionalität der IT-Basisinfrastruktur ergeben.

3.1 Fehlerhafte Systemzeit

Die Basisinfrastruktur stellt die Zeit für die De-Mail-Dienste zur Verfügung. Dabei gilt, dass De-Mail die gesetzliche Zeit verwendet. Es ist denkbar, dass durch bewusste Manipulation oder durch technisches Versagen eine falsche Zeit verwendet wird. Dies kann dazu führen, dass fehlerhafte Bestätigungen über den Zustand einer De-Mail-Nachricht ausgestellt werden.

3.2 Fehlerhafte Eintragungen im ÖVD

Fehlerhafte Einträge im ÖVD können durch Fehleingabe, technisches Versagen oder bewusste Manipulation entstehen. Solche fehlerhaften Einträge können dazu führen, dass Nachrichten an einen anderen Benutzer adressiert bzw. versendet werden und es damit zu einem Verlust hinsichtlich der Vertraulichkeit kommt.

3.3 Automatisierte ÖVD-Abfrage

Durch automatisierte Abfrage besteht die Möglichkeit, den gesamten Datenbestand des ÖVD abzufragen und danach für unbekannte Zwecke zu verwenden.

3.4 Unberechtigter Zugriff auf den ÖVD

Es besteht die Gefahr, dass unberechtigte Personen versuchen, Zugriff auf die im ÖVD verfügbaren Daten zu erlangen.

3.5 Fehlerhafte Einträge im DNS

Fehlerhafte Einträge im DNS können durch Fehleingaben, technisches Versagen oder bewusste Manipulation entstehen. Solche fehlerhaften Einträge können dazu führen, dass es zu Fehlfunktionen kommt.

4 Sicherheitsziele

Im Folgenden werden weitergehende Sicherheitsziele der IT-Basisinfrastruktur beschrieben, die über die in [TR DM Si ÜK] Aufgeführten gelten.

4.1 Verwendung der korrekten Zeit

In den Systemen muss die korrekte Zeit eingesetzt werden, um den Zeitpunkt des Eingangs und der Weiterleitung von Nachrichten genau dokumentieren zu können.

4.2 Korrekte Einträge innerhalb des ÖVD

Die Inhalte des ÖVD müssen mit den Daten des Accountmanagements übereinstimmen.

4.3 Korrekte Authentisierung der Nutzer

Eine Nutzung und Administration darf nur durch authentisierte und autorisierte Personen erfolgen.

4.4 Korrekte Einträge im DNS

Die Einträge im DNS des DMDA müssen korrekt sein.

5 Anforderungen

5.1 Allgemeine Anforderungen

5.1.1 Zeitservice

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 ist ein getrenntes Netz und 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.

5.1.2 ÖVD

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.

5.2 Administration des DNS

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