Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Dokumentenablage IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 5.3
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 DA anzuwenden sind, und ist Bestandteil von [TR DM DA M]. Dies gilt, sofern die DA angeboten wird.

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-Sicherheitskonzeptes sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt das Modul [TR DM Si M].

2.1 Erfassung des IT-Verbundes

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

3 Bedrohungen

Es gelten die in [TR DM Si ÜK] formulierten Bedrohungen, sowie weitere speziell für die DA geltenden Aspekte.

3.1 Verlust der Vertraulichkeit

Der Verlust der Vertraulichkeit wird bereits in [TR DM Si ÜK] berücksichtigt. Die Gefahr des Verlustes der Vertraulichkeit besteht im Fall der Dokumentenablage auf unterschiedlichen Ebenen:

- durch den Zugriff von Administratoren, auf die Daten oder auf die Suchindizes, die eine Suche in den Daten ermöglichen,
- durch den Diebstahl von Speichermedien.

3.2 Verlust der Integrität

Der Verlust der Integrität betrifft in diesem Zusammenhang zum einen die Manipulation von Daten durch Unbefugte und zum anderen die Veränderung der Daten durch technisches Versagen.

3.3 Verlust der Verfügbarkeit

Der Verlust der Verfügbarkeit betrifft in diesem Zusammenhang zum einen die Nicht-Erreichbarkeit des Dienstes insgesamt sowie die Verfügbarkeit der in der Dokumentenablage abgelegten Daten. Eine unberechtigte Löschung der Daten kann z. B. dazu führen, dass der Nutzer nicht mehr auf seine Daten zugreifen kann.

4 Sicherheitsziele

Es gelten die Sicherheitsziele, die in [TR DM Si ÜK] formuliert wurden.

5 Anforderungen

5.1 Kryptokonzept

Da die Speicherung personenbezogener Daten durch den Nutzer ein wesentlicher Zweck der Dokumentenablage ist, sind besondere Maßnahmen bei der Speicherung zu ergreifen. Es sind daher neben den Anforderungen aus [TR DM Si ÜK] zum Kryptokonzept, die nachfolgenden Anforderungen an die Dokumentenablage umzusetzen.

5.1.1 Vertrauliche Speicherung der Daten

Die Speicherung sämtlicher vom Nutzer eingestellter Daten auf den Systemen des DMDA hat verschlüsselt zu erfolgen.

Die Verschlüsselung der Daten hat so früh wie möglich nach Eingang auf den Systemen des DMDA zu erfolgen.

Danach darf eine Entschlüsselung der Daten nur automatisiert erfolgen und ausschließlich

- zur Prüfung auf Viren oder Schadsoftware und
- zur Auslieferung an den Nutzer.

Die Verschlüsselung kann mit einem Schlüssel für alle Nutzer erfolgen.

Es gelten folgende Regelungen für die Daten hinsichtlich

- langfristiger Speicherung (z.B. Daten in der DA):
  - Die Daten müssen einzeln oder in einem Container verschlüsselt gespeichert werden.
- kurzfristiger Speicherung (z.B. in Warteschlange bei Virenscanner):
  - Das Dateisystem, auf dem die Daten abgelegt werden, muss verschlüsselt sein.

Bei der Erstellung von Suchindizes, für die Suche innerhalb der in der DA abgelegten Daten sind diese ebenfalls verschlüsselt abzulegen.

5.1.2 Integere Speicherung der Daten

Die Speicherung der Daten auf den Systemen des DMDA hat unverfälscht zu erfolgen.

Dazu muss die Integritätssicherung der Daten so früh wie möglich nach Eingang auf den Systemen des DMDA erfolgen.

Die Integritätsprüfung erfolgt bei der Speicherung sowie beim Abruf der Daten.

5.2 Backup-Konzept

Maßnahmen zur Sicherung der Daten sind in zu berücksichtigen (vgl. [TR DM Si ÜK]).