Bundesamt
für Sicherheit in der
Informationstechnik



**EMPFEHLUNG: INTERNET-DIENSTLEISTER**

# Diskussionspapier: Absicherung von Telemediendiensten

## Nach Stand der Technik

Mit dem IT-Sicherheitsgesetz soll die Sicherheit informationstechnischer Systeme (IT-Systeme) signifikant verbessert werden. Die Neuregelungen dienen dazu, den Schutz der IT-Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu erhöhen, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können.

Im Zusammenhang mit dem IT-Sicherheitsgesetz wurde auch eine Änderung des Telemediengesetzes (TMG) vorgenommen, die die Verantwortlichen von geschäftsmäßig angebotenen Telemedien bei der Absicherung ihrer IT-Systeme stärker in die Pflicht nimmt (siehe § 13 Abs. 7 TMG):

> *Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass*
>
> *1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und*
>
> *2. diese*
>
> *a) gegen Verletzungen des Schutzes personenbezogener Daten und*
>
> *b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,*
>
> *gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen.*

Dieses Dokument richtet sich an die Adressaten des §13 Abs. 7 TMG und gibt Empfehlungen, welche Maßnahmen nach dem Stand der Technik zu berücksichtigen sind. Dazu werden im ersten Schritt die verschiedenen Provider-Typen von Telemediendiensten nach TMG erläutert. Im zweiten Schritt werden anschließend anhand von Anwendungsfällen für jeden Provider-Typ die zu berücksichtigenden Maßnahmen dargestellt.

## 1. Provider-Typen von Telemediendiensten

Unter den Begriff des Telemediendiensteanbieters des TMG lassen sich vier verschiedene Provider-Typen fassen: Content Provider, Host Provider, Access-Provider und Cache Provider. Im Folgenden werden diese Provider anhand von Beispielen beschrieben.

| Provider-Typ | Beschreibung und Beispiel |
|---|---|
| **Content Provider** – Anbieten eigener Inhalte | Stellen eigene Inhalte zum Abruf im Internet zur Verfügung.<br><br>**Beispiel:** Ein Unternehmen veröffentlicht eine eigene Website (und stellt damit Informationen zur Nutzung bereit). |
| **Host Provider** – Speichern fremder Inhalte | Stellen ein System für Dritte (z. B. für Content Provider) zur Verfügung (z. B. einen Shared-Host[1]).<br><br>**Beispiel:** Ein Unternehmen A bietet das Veröffentlichen von fremden Websites auf seinen Shared-Hosts an. Ein Unternehmen B nutzt einen Shared-Host von Unternehmen A. Damit wird Unternehmen A zum Host Provider des Unternehmens B. |
| **Access Provider** – Vermittelt den Zugang zu den Inhalten | Vermitteln mit Hilfe einer technischen Infrastruktur (z. B. einem Rechenzentrum) für Dritte (z. B. für Host Provider) den Zugang zu Inhalten.<br><br>**Beispiel:** Ein Unternehmen A stellt den Zugang zu seinem Kommunikationsnetz sowie zum Rechenzentrum zur Verfügung. Ein Unternehmen B nutzt das Kommunikationsnetz von Unternehmen A, indem es einen Server im Rechenzentrum (z. B. Co-Location) von Unternehmen A betreibt. Damit wird Unternehmen A zum Access Provider des Unternehmens B. |
| Sonderfall:<br>**Cache Provider**[2] – Zwischenspeicherung fremder Inhalte | Vermitteln mit Hilfe einer technischen Infrastruktur für Dritte den *beschleunigten* Zugang zu Inhalten.<br><br>**Beispiel:** Ein Unternehmen (z. B. ein Content Delivery Network) unterhält ein System, um Inhalte effizienter auszuliefern. Dadurch nimmt das Unternehmen üblicherweise die beiden Rollen Access Provider und Host Provider ein, da es ein Kommunikationsnetz und Server zur Verfügung stellt, um die gespiegelten Inhalte eines Content Providers effizient ausliefern zu können. |

Tabelle 1: Provider-Typen von Telemediendiensten

Zum Betrieb eines vollständigen Telemediendienstes muss mindestens ein Content, ein Host und ein Access Provider vorhanden sein (vgl. blaue Kästen in Abbildung 1). Ein Sonderfall ist der Cache Provider, der sowohl die Rolle des Host als auch des Access Providers einnimmt. Aus technischer Sicht müssen also mindestens Inhalte (z. B. HTML-Dateien), eine Anzahl von Servern (z. B. ein Web-Server) und eine Infrastruktur (z. B. ein Router mit Internetzugang) zur Verfügung stehen, damit ein Telemediendienst vollständig und funktionsfähig ist. Alle drei Rollen (Content, Host und Access Provider) können hierbei in einer Person zusammenfallen oder einzelne Rollen an andere Unternehmen auslagert werden.

1 Auf einem Shared-Host werden die Websites mehrerer Kunden auf einem einzelnen Web-Server betrieben.
2 Die Maßnahmen für einen Cache Provider werden in diesem Dokument nicht separat berücksichtigt, da er grundsätzlich die Funktionen eines Host- und Access-Provider besetzt..

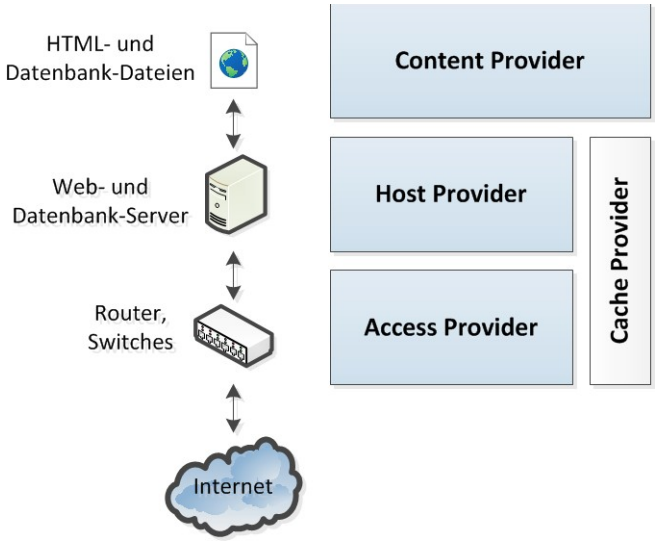


Abbildung 1: Modell eines vollständigen Telemediendienstes.

# 2. Maßnahmen zur Absicherung

In diesem Abschnitt werden für jeden Provider-Typ (siehe Abschnitt 1) die aus Sicht des BSI dazugehörigen Sicherheitsmaßnahmen zur Absicherung nach Stand der Technik in einer Tabelle (siehe Tabelle 2) beschrieben. Zunächst wird der strukturelle Aufbau dieser Tabelle und anschließend die praktische Anwendung der Tabelle erläutert.

## 2.1. Aufbau der Tabelle

### a) Provider-Typen

In der ersten Spalte der Tabelle sind die verschiedenen Provider-Typen (Content-, Host- und Access-Provider) aufgelistet. Die Maßnahmen für den entsprechenden Provider-Typ sind so gewählt, dass diese innerhalb dessen Eingriffsmöglichkeiten technisch und organisatorisch umsetzbar sind.

### b) Maßnahmen

In der zweiten bzw. dritten Spalte der Tabelle sind für jeden Provider-Typ die dazugehörigen Basis- bzw. Standard-Maßnahmen nach Stand der Technik aufgeführt. Basis-Maßnahmen MÜSSEN grundsätzlich umgesetzt werden. Standard-Maßnahmen SOLLTEN zusätzlich umgesetzt werden.

Bei der Umsetzung der Maßnahmen ist die für den jeweiligen verantwortlichen Provider wirtschaftliche Zumutbarkeit zu beachten. Die Zumutbarkeit muss im Einzelfall beurteilt werden.

Die in der Tabelle aufgeführten Maßnahmen zur Absicherung des Telemediendienstes werden im Anschluss erläutert. Des Weiteren werden zu jeder Maßnahme weiterführende Informationen zur Umsetzung angegeben (mit Referenzen zum IT-Grundschutz, zu Dokumenten der ISi-Reihe und zu Sicherheitsempfehlungen der Allianz für Cybersicherheit).

## 2.2. Anwendung der Tabelle

Ein Telemediendienst setzt sich in seiner Gesamtheit aus Inhalten, Server und Infrastruktur zusammen. Die zu berücksichtigenden Sicherheitsmaßnahmen umfassen somit die einzelnen Maßnahmen zur Absicherung der Inhalte, der Server und der Infrastruktur. Werden Teile des Telemediendienstes an andere Unternehmen ausgegliedert (z. B. an einen Host Provider oder an einen Access Provider), sorgt der für den Telemediendienst verantwortliche Provider dafür (etwa durch vertragliche Regelungen), dass die Maßnahmen durch das beauftragte Unternehmen in seinem Zuständigkeitsbereich umgesetzt werden.

Im Folgenden wird die Anwendung der Tabelle anhand von verschiedenen Anwendungsfällen beispielhaft erläutert. Das Ziel der Beschreibung von Anwendungsfällen ist, die unterschiedlichen Verantwortlichkeiten darzustellen: Welche Maßnahmen muss der Provider selber berücksichtigen und welche Maßnahmen muss der Provider (z. B. vertraglich) sicherstellen.

**Anwendungsfall 1:** Ein Unternehmen A hostet seine Website bei einem Unternehmen B, das auch die Infrastruktur zur Verfügung stellt. Dadurch wird das Unternehmen A zum Content Provider. Das Unternehmen B wird zu einem Host Provider und zu einem Access Provider und muss verpflichtet werden, die entsprechenden Maßnahmen für das „Speichern von Inhalten" und für das „Durchleiten von Inhalten" umzusetzen.

**Anwendungsfall 2:** Ein Unternehmen A bietet das Hosten von fremden Websites an. Dadurch wird das Unternehmen A zum Host Provider und muss die Maßnahmen für das „Speichern von Inhalten" berücksichtigen. Betreibt das Unternehmen A gleichzeitig einen eigenen Internetzugang, wird es zusätzlich zum Access Provider und muss die Maßnahmen für das „Durchleiten von Inhalten" berücksichtigen. Benutzt das Unternehmen A die Leistungen von Unternehmen B, dann muss Unternehmen A (z. B. vertraglich) sicherstellen, dass Unternehmen B die entsprechenden Maßnahmen berücksichtigt.

**Anwendungsfall 3:** Ein Unternehmen hostet seine Website auf einem eigenen Web-Server am eigenen DSL-Anschluss. Dadurch wird das Unternehmen zum Content Provider (da es Inhalte anbietet), zum Host Provider (da es Inhalte speichert) und zum Access Provider (da es Inhalte durchleitet). Das Unternehmen muss deshalb die Maßnahmen für das „Anbieten von Inhalten", das „Speichern von Inhalten" sowie für das „Durchleiten von Inhalten" berücksichtigen.

**Anwendungsfall 4:** Ein Unternehmen A hostet seine Website auf einem Root-Server in einem Rechenzentrum von einem Unternehmen B. Dadurch wird das Unternehmen A zum Content Provider und zum Host Provider. Das Unternehmen B wird zum Access Provider. Das Unternehmen A muss die Maßnahmen für das „Anbieten von Inhalten" sowie für das „Speichern von Inhalten" berücksichtigen. Das Unternehmen B muss die Maßnahmen für das „Durchleiten von Inhalten" berücksichtigen. Handelt es sich bei dem Root-Server jedoch um ein virtuelles System, so muss Unternehmen B bei der Absicherung des Servers von Unternehmen A unterstützen, da es Teil des Host Providers ist.

**Anwendungsfall 5:** Ein Unternehmen A hostet seine Website bei einem Unternehmen B. Des Weiteren stellt das Unternehmen A auf seiner Website einen Bereich zur Verfügung, auf dem ein Werbebanner eingeblendet werden kann. Unternehmen A überlässt Unternehmen C, Werbebanner auszuwählen und in dem zur Verfügung stehenden Bereich einzublenden. Damit sind Unternehmen A und Unternehmen C Content Provider der Website von Unternehmen A. Des Weiteren sollte das Unternehmen A das Unternehmen C vertraglich verpflichten, die Maßnahmen für Content Provider umzusetzen.

## 2.3. Tabelle der Sicherheitsmaßnahmen

| Provider-Typ | Basis-Maßnahmen | Standard-Maßnahmen |
|---|---|---|
| **Content Provider**<br>Anbieten von Inhalten | M.01 Sichere Passwörter<br>M.02 Sicherheits-Updates<br>M.03 Gehärtete Konfiguration<br>M.04 Datensicherung<br>M.05 Virenschutz<br>M.06 Firewall<br>M.08 Anwendungssicherheit<br>M.17 Zugriffskontrolle | M.07 Verschlüsselung<br>M.09 Monitoring<br>M.10 Kompatibilitätstest<br>M.11 Redundanz<br>M.14 Mitarbeiter-Sensibilisierung<br>M.15 Regelung der Verantwortlichkeiten<br>M.16 Hersteller-Unterstützung |
| **Host Provider**<br>Speichern von Inhalten<br><br>z. B.<br>Shared-Hosts, Root-Server | M.01 Sichere Passwörter<br>M.02 Sicherheits-Updates<br>M.03 Gehärtete Konfiguration<br>M.04 Datensicherung<br>M.06 Firewall<br>M.07 Verschlüsselung<br>M.08 Anwendungssicherheit<br>M.09 Monitoring<br>M.16 Hersteller-Unterstützung<br>M.17 Zugriffskontrolle<br>M.18 Zutrittskontrolle | M.05 Virenschutz<br>M.10 Kompatibilitätstest<br>M.11 Redundanz<br>M.12 DDoS-Mitigation<br>M.13 Sicherheits- und Notfallvorsorge-Konzept<br>M.14 Mitarbeiter-Sensibilisierung<br>M.15 Regelung der Verantwortlichkeiten<br>M.19 Penetrationstests und IS-Revisionen |
| **Access Provider**<br>Vermittlung des Zugangs zu Inhalten<br><br>z. B.<br>Infrastruktur, Internetzugang | M.01 Sichere Passwörter<br>M.02 Sicherheits-Updates<br>M.03 Gehärtete Konfiguration<br>M.04 Datensicherung<br>M.07 Verschlüsselung<br>M.08 Anwendungssicherheit<br>M.09 Monitoring<br>M.16 Hersteller-Unterstützung<br>M.17 Zugriffskontrolle<br>M.18 Zutrittskontrolle | M.06 Firewall<br>M.10 Kompatibilitätstest<br>M.11 Redundanz<br>M.12 DDoS-Mitigation<br>M.13 Sicherheits- und Notfallvorsorge-Konzept<br>M.14 Mitarbeiter-Sensibilisierung<br>M.15 Regelung der Verantwortlichkeiten<br>M.19 Penetrationstests und IS-Revisionen |

Tabelle 2: Sicherheitsmaßnahmen

## 2.4. Sicherheitsmaßnahmen

In Kapitel 2.5 werden die empfohlenen Maßnahmen zur Absicherung von Telemediendiensten gegen unerlaubten Zugriff auf die technischen Einrichtungen, Verletzung des Schutzes personenbezogener Daten sowie Störungen beschrieben. Zusätzlich zu diesen Sicherheitsmaßnahmen müssen bei Umgang mit personenbezogenen Daten die datenschutzrechtlichen Anforderungen eingehalten werden, die hiervon unberührt sind. Hilfestellungen dazu findet man in folgenden Referenzen:

- ➔ IT-Grundschutz B 1.5
- ➔ IT-Grundschutz M 1.16
- ➔ IT-Grundschutz M 2.501 ff

Die Sicherheitsmaßnahmen zur Absicherung von Telemediendiensten aus Tabelle 2 werden in den jeweiligen Abschnitten kurz erläutert und enthalten zudem Referenzen zum IT-Grundschutz, zur ISi-Reihe oder zu Sicherheitsempfehlungen der Allianz für Cybersicherheit.

Die folgenden Referenzen beziehen sich zunächst allgemein auf das Absichern von Telemediendiensten und sind als ergänzende Hilfestellungen anzusehen:

a) **ISi-Reihe**
   - ➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
   - ➔ Absicherung eines Servers (ISi-Server)

b) **Sicherheitsempfehlungen der Allianz für Cybersicherheit**
   - ➔ #6: Basismaßnahmen der Cyber-Sicherheit
   - ➔ #41: Bereitstellung von Webangeboten
   - ➔ #68: Sicheres Webhosting: Handlungsempfehlungen für Webhoster
   - ➔ #115: Schützen Sie sich vor professionellen gezielten Cyber-Angriffen

c) **Open Web Application Security Project (OWASP)**
   - ➔ OWASP Top Ten Project
   - ➔ OWASP Cheat Sheet Series

### 2.5. Beschreibung der Sicherheitsmaßnahmen

*M.01 Sichere Passwörter*

Verwendet der Provider von Telemediendiensten Passwörter zur Authentisierung (z. B. für Benutzer und Administratoren), so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung entscheidend davon abhängig, ob die Passwörter korrekt gebraucht werden. Deshalb müssen durch das Definieren von Richtlinien sichere Passwörter etabliert werden. Beispielsweise müssen die Passwörter hinreichend stark gegenüber Brute-Force-Angriffen sein.

Beispiele:

- für Content-Provider: Sichere Passwörter für die Blog- oder CMS-Software.
- für Host-Provider: Sichere Passwörter für die Web- und Datenbank-Server.
- für Access-Provider: Sichere Passwörter für Netzwerkkomponenten.

Referenzen:

- ➔ IT-Grundschutz M 2.11

*Hinweis:* Werden im Telemediendienst vertrauliche oder sensible Informationen übertragen (z. B. personenbezogene Daten oder Authentisierungsdaten), dann dürfen Passwörter nur mit einer Transportverschlüsselung übertragen werden (→ siehe Standard-Maßnahme „M.07 Verschlüsselung“). Des Weiteren sollte für die Administration des Telemediendienstes eine Mehrfaktor-Authentisierung berücksichtigt werden, um einen wirksamen Schutz gegen gestohlene Passwörter zu bieten.

*M.02 Sicherheits-Updates*

Provider von Telemediendiensten verwenden zum Betrieb verschiedene Software-Komponenten (z. B. Blog- oder CMS-Software und deren Erweiterungen). Angreifer könnten Schwachstellen in diesen Komponenten ausnutzen. Durch Sicherheits-Updates können bekannte Schwachstellen beseitigt werden und müssen daher im Rahmen eines Patchmanagement-Prozesses schnellstmöglich eingespielt werden.

Beispiele:

- für Content-Provider: Sicherheits-Updates für Blog- oder CMS-Software und deren Er-

weiterungen.

- für Host-Provider: Sicherheits-Updates für Betriebssysteme, Web-Server (z. B. Apache, IIS) und Datenbank-Server (z. B. MySQL, PostgreSQL).
- für Access-Provider: Sicherheits-Updates für Netzwerkkomponenten.

Referenzen:

- ➔ Sicherheitsempfehlung der Allianz für Cybersicherheit: #93: Management von Schwachstellen und Sicherheitsupdates
- ➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
- ➔ IT-Grundschutz M 4.83
- ➔ IT-Grundschutz B 1.14

*M.03 Gehärtete Konfiguration*

Bei der Härtung eines IT-Systems werden alle Funktionen deaktiviert, die zur Erfüllung des vorgesehenen Dienstes nicht erforderlich sind. Die benötigten Einstellungen müssen unter Sicherheitsgesichtspunkten überprüft werden. Dazu können beispielsweise die „Hardening Guides" der entsprechenden Hersteller (z. B. Apache HTTP Server) genutzt werden. Für potentielle Angreifer ergibt sich dadurch eine geringere Angriffsfläche.

Beispiele:

- für Content-Provider:
  - Deaktivierung nicht benötigter Erweiterungen in der Blog- oder CMS-Software.
  - Vermeidung der Preisgabe von Informationen, z. B. durch Deaktivierung detaillierter Fehlermeldungen (sofern dies technisch möglich ist).
- für Host- und Access-Provider:
  - Deaktivierung von nicht benötigten Server- oder Netzwerk-Diensten.
  - Vermeidung der Preisgabe von Informationen, z. B. durch Deaktivierung detaillierter Fehlermeldungen (sofern dies technisch möglich ist).
  - Härtung der Betriebssysteme.

Referenzen:

- ➔ Apache HTTP Server Security Tips
- ➔ Absicherung eines Servers (ISi-Server)

*M.04 Datensicherung*

Zur Vermeidung von Datenverlusten und der Sicherstellung der Verfügbarkeit des Telemediendienstes müssen regelmäßig, und wenn möglich automatisiert, Datensicherungen durchgeführt werden. Datensicherungen müssen so vorgehalten werden, dass kein permanenter Schreibzugriff darauf möglich ist (z. B. Offline-Kopien). Beispielsweise existieren Varianten von „Ransomware", die Dateien auf Netzwerkfreigaben verschlüsseln – auch wenn diese momentan im Dateisystem nicht eingehängt sind. Generell ist ohne Datensicherung im Falle einer Kompromittierung keine Wiederherstellung möglich. Des Weiteren stellt die Datensicherung Voraussetzung für die Standard-Maßnahme „M.13 Sicherheits- und Notfallvorsorge-Konzept" dar.

Beispiele:

- für Content-Provider: Sicherung der Inhalte der Website (u. a. Text- und Grafikdateien) sowie der Datenbank (z. B. als „SQL-Dump“).
- für Host- und Access-Provider: Sicherung der Konfiguration von Servern und Netzwerkkomponenten.

Referenzen:

➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)

➔ IT-Grundschutz M 6.32

➔ IT-Grundschutz B 1.4

*M.05 Virenschutz*

Zum Schutz vor Schadprogrammen in Telemediendiensten sollten Virenschutz-Programme eingesetzt werden. Diese können nach bekannten Schadprogrammen suchen und sie gleichzeitig isolieren oder entfernen.

Beispiele:

- für Content-Provider: Einsatz eines Virenschutz-Programms auf dem lokalen System, um die Inhalte vor dem Hochladen zum Host-Provider zu überprüfen.
- für Host-Provider: Einsatz eines Virenschutz-Programms auf den Web-Servern, um schadhafte Inhalte beispielsweise schon beim Hochladen aufspüren zu können (sofern dies technisch möglich und sinnvoll ist).

Referenzen:

➔ IT-Grundschutz M 4.3

➔ IT-Grundschutz B 1.6

*M.06 Firewall*

Durch den Anschluss an das Internet sind Telemediendienste vielen Gefährdungen ausgesetzt. Beispielsweise könnten durch einen Angriff Daten aus einem internen Netz in das Internet unbefugt abfließen. Firewalls (bzw. Sicherheitsgateways) kontrollieren und ggf. unterbinden Zugriffe auf einen Telemediendienst und müssen als effektiver Schutz für den Telemediendienst eingesetzt werden.

Beispiele:

- für Content-Provider: Einsatz einer Personal Firewall auf dem lokalen System, das die Inhalte zum Host-Provider hochlädt. In vielen aktuellen Betriebssystemen ist eine Personal Firewall bereits integriert.
- für Host-Provider: Einsatz von IP-Tables (oder ähnliche Funktion) auf den Server-Systemen.
- für Access-Provider: Einsatz einer zustandsbehafteten Firewall, die mindestens IP- und Portbereiche filtern kann.

Referenzen:

➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)

➔ Sicherheitsempfehlung der Allianz für Cybersicherheit:
#112: Next Generation Firewalls

➔ IT-Grundschutz M 2.70 ff

*M.07 Verschlüsselung*

Werden bei Telemediendiensten vertrauliche oder sensible Informationen übertragen oder gespeichert, besteht die Möglichkeit, dass diese Informationen Unbefugten zur Kenntnis gelangen und von diesen manipuliert werden. Aus diesem Grund sollte ein Verschlüsselungsverfahren nach Stand der Technik zum Schutz der Daten eingesetzt werden, um die Vertraulichkeit und die Integrität der Telemedien sicherzustellen.

Hierbei kann zwischen der Verschlüsselung der Daten für den Transport und für die Speicherung unterschieden werden. Für den verschlüsselten Transport von Daten (z. B. der Datenverkehr zwischen Web-Server und Client) sollte das SSL/TLS-Protokoll (hier: HTTPS) eingesetzt werden. Für die verschlüsselte Speicherung von Daten (z. B. die Passwörter des Telemediendienstes) sollte eine sichere Hashfunktion benutzt werden. Hierzu wird auf die technischen Richtlinien „BSI TR-02102-1“ und „BSI TR-02102-2“ des BSI verwiesen.

Beispiele:

- für Content-Provider:
  - Nutzung von HTTPS zur Auslieferung von Inhalten (z. B. bei einem Online-Shop).
- für Host-Provider:
  - Nutzung von SSH oder anderen Transportverschlüsselungen zur Konfiguration der Web-und Datenbank-Server.
- für Access-Provider:
  - Nutzung von SSH oder anderen Transportverschlüsselungen zur Administration von Netzwerkkomponenten.

Referenzen:

➔ Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls

➔ Migrationsleitfaden zum Mindeststandard des BSI

➔ BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

➔ BSI TR-02102-2 Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)

➔ Sicherheitsempfehlung der Allianz für Cybersicherheit:
#12: TLS/SSL Best Practice v2.0 - Allianz für Cyber-Sicherheit

➔ IT-Grundschutz M 4.34

➔ IT-Grundschutz B 1.7

*M.08 Anwendungssicherheit*

Viele Telemediendienste, z. B. Web-Anwendungen wie Online-Shops, verwenden im Hintergrund Zwischenanwendungen („Middleware“) und/oder Datenbanken zur Verarbeitung und Speicherung von Inhalten. Diese Zwischenanwendungen sind meistens eng mit dem Web-Server verbunden und damit potentiellen Angriffen ausgesetzt. Aus diesem Grund müssen die

eingesetzten Web-Anwendungen, Zwischenanwendungen und Datenbanken sicher konfiguriert werden.

Beispiele:

- für Host- und Access-Provider: Zugriffskontrolle der Datenbank (z. B. Zugriff auf die Datenbank ist nur von bestimmten Servern möglich).

Referenzen:

➔ IT-Grundschutz M 4.69

*Input-/Output-Validierung:* Alle an eine Web-Anwendung und Zwischenanwendung übergebenen Daten müssen als potenziell gefährlich behandelt und entsprechend gefiltert werden. Durch eine zuverlässige und gründliche Filterung der Ein- und Ausgabedaten mittels einer Validierungskomponente kann ein wirksamer Schutz vor gängigen Angriffen erreicht werden. Hierbei sollten sowohl die Eingabedaten von Benutzern als auch die Ausgabedaten der Web-Anwendung an die Clients gefiltert werden.

➔ IT-Grundschutz M.4.393

*Session-Management:* Beinhaltet der Telemediendienst eine Web-Anwendung, so verwendet er in der Regel das zustandslose HTTP-Protokoll zur Übertragung der Daten. Um zusammengehörende Anfragen zu erkennen und deren Daten zusammenzufügen, muss eine sogenannte Session verwendet werden. Das Session-Management einer Website hat zur Aufgabe, die Sessions zu verwalten. Dabei sollten die folgenden Anforderungen berücksichtigt werden:

➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server) (Abschnitt 4.2.6)

*M.09 Monitoring*

In Telemediendiensten sollten sicherheitsrelevante Aktivitäten (im Rahmen der gesetzlichen Bestimmungen) protokolliert werden. Dadurch ist es möglich, Angriffe auf den Telemediendienst zu erkennen und nachzuverfolgen, um einen besseren Schutz der Daten gewährleisten zu können. Hierbei ist zu beachten, dass der gesetzliche Datenschutz eingehalten werden muss.

Beispiele:

- für Content-Provider:
  - Protokollierung der Zugriffe auf den Blog oder das CMS (in vielen Produkten konfigurierbar).
- für Host-Provider:
  - Protokollierung der Anfragen an den Web-Server.
- für Access-Provider:
  - Aktivierung von Firewall-Logs.

Referenzen:

➔ Absicherung eines Servers (ISi-Server)

➔ IT-Grundschutz M 2.500

➔ IT-Grundschutz M 5.71

*M.10 Kompatibilitätstest*

Wird im Telemediendienst eine neue Komponente (z. B. eine neue Software) eingesetzt, sollte diese vor Inbetriebnahme in einer Testumgebung überprüft werden. Beispielsweise sollte ein Kompatibilitätstest die Verträglichkeit mit vorhandenen Standards überprüfen. Dadurch wird sichergestellt, dass sich die neue Komponente nicht negativ (z. B. durch Software-Bugs) auf den Telemediendienst auswirkt.

Beispiele:

- für Content-Provider: Testen von selbst entwickelten Skripten.
- für Host-Provider: Test eines Betriebssystem-Updates.
- für Access-Provider: Test eines neuen Switches.

Referenzen:

➔ Sicherheitsempfehlung der Allianz für Cybersicherheit:
#22: Entwicklung sicherer Webanwendungen

➔ IT-Grundschutz M 4.65

➔ IT-Grundschutz B 1.14

*M.11 Redundanz*

Der Betreiber eines Telemediendienstes sollte dessen Verfügbarkeit sicherstellen. Dies kann durch die Bereitstellung von redundanten Komponenten erreicht werden. Redundanz bedeutet hier, dass funktional gleiche oder vergleichbare Ressourcen eines Telemediendienstes vorhanden sind, beispielsweise eine Unterbrechungsfreie Stromversorgung (USV) oder ein Content-Delivery-Network (CDN). Bei der Umsetzung solcher Maßnahmen ist die wirtschaftliche Zumutbarkeit zu berücksichtigen und einzelfallabhängig zu beurteilen.

Beispiele:

- für Content-Provider:
  - Bereitstellung eines Ersatz-Rechners.
  - Mehrfach abgesicherte Aufstellung der Content-Dienste (z. B. Webserver)
- für Host- und Access-Provider:
  - Doppelte Server- und Netzwerkkomponenten.
  - Mehrere Internetzugänge.

Referenzen:

➔ Hochverfügbarkeitskompendium

➔ IT-Grundschutz M 1.70

➔ IT-Grundschutz M 1.52

*M.12 DDoS-Mitigation*

Es existieren verschiedene Arten von DDoS-Angriffen. Beispielsweise könnte der Telemediendienst mit einer größeren Anzahl von Anfragen, als die er verarbeiten kann, überflutet werden. Dadurch können reguläre Anfragen nicht mehr beantwortet werden, sodass der Telemedien-

dienst nicht mehr verfügbar ist. Der Telemediendienst sollte DDoS-Angriffe abwehren können, in dem beispielsweise alle IP-Pakete, deren Quelladresse im Bereich der angreifenden IP-Adressen liegt, am Router verworfen werden. Bei der Umsetzung solcher Maßnahmen ist die wirtschaftliche Zumutbarkeit zu berücksichtigen und einzelfallabhängig zu beurteilen.

Referenzen:

- ➔ Themenseite zu DDoS der Allianz für Cybersicherheit

*M.13 Sicherheits- und Notfallvorsorge-Konzept*

Der Telemediendienst sollte über ein Sicherheits- und Notfallvorsorge-Konzept verfügen, indem festgelegt wird, welche Ziele und Strategien bzgl. der Informationssicherheit verfolgt werden sollen. Dazu gehört beispielsweise die Feststellung des Schutzbedarfs, die Auswahl und Anpassung von Sicherheitsmaßnahmen sowie die Bestimmung eines IT-Sicherheitsbeauftragten. Des Weiteren sollte das Notfallvorsorge-Konzept einen wichtigen Aspekt des Sicherheitskonzeptes darstellen. Mit einem Notfallvorsorge-Konzept kann sichergestellt werden, dass bei Sicherheitsvorfällen (z. B. bei entdeckten Sicherheitslücken) eine entsprechende Notfallvorsorge vorhanden ist. Beispielsweise könnte der Telemediendienst an ein Computer Emergency Response Team (CERT) angeschlossen werden oder selber über ein solches verfügen.

Zusammengefasst sollte der Telemediendienst über ein „Information Security Management System“ (ISMS) verfügen, das Regeln definiert, um die Informationssicherheit dauerhaft zu planen, umzusetzen, zu prüfen, aufrechtzuerhalten und zu verbessern.

Referenzen:

- ➔ IT-Grundschutz M 6
- ➔ IT-Grundschutz B 1.3
- ➔ IT-Grundschutz B 1.8

*M.14 Mitarbeiter-Sensibilisierung*

Sicherheitsvorfälle können durch unsachgemäßes Verhalten von Mitarbeitern eines Telemediendienstes hervorgerufen werden. Daher sollte sichergestellt werden, dass alle Mitarbeiter ausreichende Fachkenntnisse in der Informationssicherheit haben. Dazu gehört beispielsweise, sich fortlaufend über das Thema IT-Sicherheit zu informieren.

Referenzen:

- ➔ IT-Grundschutz M 2.197 ff
- ➔ IT-Grundschutz M 3.5
- ➔ IT-Grundschutz B 1.13

*M.15 Regelung der Verantwortlichkeiten*

In vielen Fällen wirken viele beteiligte Personen an einem Telemediendienst mit, z. B. Mitarbeiter und externe Auftragnehmer. Aus diesem Grund sollten die internen und externen personellen Verantwortlichkeiten geregelt werden. Dazu sollte festgelegt werden, welche Mitarbeiter für bestimmte Maßnahmen (z. B. Datensicherung, Firewall) verantwortlich sind. Des Weiteren sollte bei der Vertragsgestaltung mit externen Auftragnehmern („Outsourcing“) darauf geachtet werden, dass Informationssicherheit in Verträgen berücksichtigt wird. Die personellen Ver-

antwortlichkeiten können im Rahmen des Sicherheitskonzeptes festgelegt werden (→ siehe Standard-Maßnahme „M.13 Sicherheits- und Notfallvorsorge-Konzept“).

Referenzen:

➔ IT-Grundschutz B 1.2

➔ IT-Grundschutz B 1.11

*M.16 Hersteller-Unterstützung*

Wurde eine Software oder eine Software-Anpassung des Telemediendienstes bei einem Hersteller in Auftrag gegeben („Customizing“), muss die Unterstützung (der Support) des Herstellers berücksichtigt werden. Dadurch soll sichergestellt werden, dass Sicherheitslücken schnellstmöglich geschlossen werden. Beispielsweise könnte es vorteilhaft sein, einen Wartungsvertrag mit dem Hersteller abzuschließen, damit dieser Sicherheits-Updates zur Verfügung stellt. Wird Open-Source-Software eingesetzt, muss überprüft werden, inwieweit die Community der entsprechenden Software weiterhin Updates bereitstellt.

Beispiele:

- für Content-Provider: Support für eingesetzte Erweiterungen in Blog- und CMS-Software.
- für Host- und Access-Provider: Support für Betriebssysteme und Netzwerkkomponenten.

Referenzen:

➔ IT-Grundschutz M 2.4

*M.17 Zugriffskontrolle*

Der Zugriff auf Software und Hardware des Telemediendienstes muss geregelt werden. Zugriffsrechte (z. B. Lesen, Schreiben, Ausführen) auf Daten sind von der Rolle abhängig, die eine Person im Rahmen des Telemediendienstes (z. B. Betreiber, Mitarbeiter, Kunde, Gast) wahrnimmt. Generell muss nach dem „principle of least privilege” gehandelt werden, d. h., dass eine Person nur die Zugriffsrechte besitzt, die sie auch tatsächlich für ihre Arbeit benötigt. Die Zugriffsrechte müssen durch die Rechteverwaltung des Systems umgesetzt werden.

Beispiele:

- für Content-Provider:
  - Zugriffsrechte für (weitere) Blog-Redakteure festlegen.
- für Host-Provider:
  - Zugriffsrechte auf Verzeichnisse des Web-Servers festlegen.
  - Web-Server mit eigenen Benutzerrechten ausstatten.
  - Gekapselte Umgebung für bestimmte Server-Dienste.
- für Access-Provider:
  - Trennung bestimmter Netzwerksegmente (Administrations-Netz, Benutzer-Netz).

Referenzen:

➔ IT-Grundschutz M 2.7

➔ IT-Grundschutz M 2.8

*M.18 Zutrittskontrolle*

Der Schutzbedarf eines Raumes (z. B. ein Server-Raum) leitet sich ab aus dem Schutzbedarf der im jeweiligen Raum verarbeiteten Informationen. Der Zutritt zu schutzbedürftigen Räumen muss deshalb geregelt und kontrolliert werden. Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu komplexen Identifizierungssystemen.

Beispiel:

- für Host- und Access-Provider: Zutrittsrechte für das Rechenzentrum festlegen.

Referenzen:

➔ IT-Grundschutz M 2.6

*M.19 Penetrationstests und IS-Revisionen*

Mit Hilfe von Penetrationstests (z. B. im Rahmen einer IS-Revision) sollte die aktuelle Sicherheit eines Telemediendienstes festgestellt werden. Sie dienen dazu, die Erfolgsaussichten eines Angriffs auf den Telemediendienst einzuschätzen und daraus notwendige Sicherheitsmaßnahmen abzuleiten (bzw. die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen).

Referenzen:

➔ Sicherheitsempfehlung der Allianz für Cybersicherheit:
#32: Durch IS-Revisionen häufig festgestellte Sicherheitsmängel

➔ IT-Grundschutz M 5.150

Dieses Dokument ist unter Beteiligung des Bitkom e.V. und des Expertenkreises Internetbetreiber der Allianz für Cyber-Sicherheit entstanden. Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **telemediendienste@bsi.bund.de** gesendet werden.