Neue Pflicht zu technisch-organisatorischen Vorkehrungen durch § 13 Abs. 7 TMG

RA Dr. Jan K. Köcher
Syndikus

DFN-CERT Services GmbH
koecher@dfn-cert.de

Hintergrund

- **IT-Sicherheitsgesetz**
  - Am 25.07.2015 in Kraft getreten
  - Erhöhung der Sicherheit informationstechnischer Systeme
    - In erster Linie Betreiber „Kritischer Infrastrukturen
    - Enthält aber auch Anforderungen an alle Betreiber von Telekommunikations- und Telemediendiensten

Kreis der Verpflichteten

- **§ 13 Abs. 7 TMG**

  Diensteanbieter ... im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien...

  - Diensteanbieter:
    - § 2 S. 1 Nr. 1 TMG: Jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält...

    → Content-Provider und Host-Provider

    ... oder den Zugang zur Nutzung vermittelt...

    → Access-Provider

Kreis der Verpflichteten

- ...im Rahmen ihrer jeweiligen Verantwortlichkeit...
- → Verweis auf Verantwortlichkeit gem. § 7 TMG
  - → Content-Provider: Grundsatz der eigenen Verantwortlichkeit für eigene Informationen
  - → Host-Provider: Nicht verpflichtet, die von ihnen gespeicherten fremden gespeicherten Informationen zu überwachen. Aber trotz Nichtverantwortlichkeit ggf. Pflicht zur Entfernung oder Sperrung der Nutzung von Informationen.
  - → Access-Provider: Wie der Host-Provider in Bezug auf die Übermittlung fremder Informationen

Kreis der Verpflichteten

- ...für geschäftsmäßig angebotene Telemedien
- Keine gesetzliche Definition und strittig:
  - Mindermeinung: Auslegung als beruflich oder gewerblich und damit nur unternehmerische Angebote mit Gewinnerzielungsabsicht.
  - Herrschende Meinung: Telemedien werden auf Grund einer nachhaltigen Tätigkeit mit oder ohne Gewinnerzielungsabsicht erbracht.
  - → Schulen und Hochschulen werden ebenfalls erfasst.

Kreis der Verpflichteten

- BT-Drucksache 18/4096, S. 34:

  „Geschäftsmäßig ist ein Angebot dann, wenn es auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt. Bei einem entgeltlichen Dienst liegt dies regelmäßig vor, so z.B. bei werbefinanzierten Webseiten. Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird demgegenüber nicht erfasst."

→ Spricht eher für die herrschende Meinung...

Pflichten

- **Durch technische und organisatorische Vorkehrungen sicherstellen, dass**
  1. kein unerlaubter Zugriff auf die für die Erbringung 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.

§ 13 Abs. 7 S. 1 Nr. 1 TMG

- **Sicherstellung, dass keine unerlaubten Zugriffe möglich sind**
  - Bezieht sich auf die zur Erbringung des Dienstes eingesetzten Systeme
  - Verhinderung von Zugriffen sowohl externer als auch interner Unbefugter

  - Rechtsfolgen:
    - Ordnungswidrigkeit mit einem Bußgeld von bis zu 50.000 €
    - Zivilrechtliche Ansprüche

§ 13 Abs. 7 S. 1 Nr. 2a TMG

- **Sicherstellung des Schutzes personenbezogener Daten**
  - Pflicht bezieht sich auf die zur Erbringung eingesetzten Systeme
  - Spezialregelung im Verhältnis zu § 9 BDSG und den entsprechenden Normen in den Landesdatenschutzgesetzen
  - Rechtsfolgen:
    - Ordnungswidrigkeit mit einem Bußgeld von bis zu 50.000 €
    - Zivilrechtliche Ansprüche

§ 13 Abs. 7 S. 1 Nr. 2b TMG

- **Sicherung gegen Störungen**
  - Pflicht bezieht sich auf die zur Erbringung eingesetzten Systeme
  - Störung?
    - → Rückgriff auf § 100 Abs. 1 TKG scheidet mangels Regelungslücke aus
    - → Früherer Entwurf:"Einwirkungen …, bei denen eine Beeinträchtigung für die Verfügbarkeit, Vertraulichkeit oder Integrität der informationsverarbeitenden Systeme … droht."
  - Bei Verstoß: Keine Ordnungswidrigkeit!

Gemeinsame Anforderungen

- **Geeignete und zur Erfüllung der Pflichten erforderliche technische und organisatorische Vorkehrungen**
  - Technische Vorkehrungen
    - z.B. Verschlüsselung, Sicherheitsupdates, Einsatz angemessener Authentifizierungsmaßnahmen.
  - Organisatorische Vorkehrungen
    - z.B. IT-Sicherheitskonzept, IT-Sicherheitsbeauftragter, organisationsinterne Regelungen zum Umgang mit personenbezogenen Daten.

Gemeinsame Anforderungen

- **„Stand der Technik“**
  - **Allgemein anerkannte Regeln der Technik**
    - stellen solche Verfahren und Ansichten dar, die sich in der technischen Praxis bewährt und durchgesetzt haben.
  - **Stand von Wissenschaft und Forschung**
    - das nach neuesten Erkenntnissen der Wissenschaft Erforderliche.
  - **Stand der Technik (Begriff BSI-Gesetz)**
    - Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.

Gemeinsame Anforderungen

- **Was bedeutet dies für einzelne Maßnahmen und Maßnahmebündel?**
- **Leitfäden durch Verbände**
  - z.B. TeleTrust Handreichung zum Begriff „Stand der Technik“ Link: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
  - BSI zusammen mit BITKOM
  - Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik
  - Weiterentwicklung zu einer Cyber-Sicherheitsempfehlung geplant

Gemeinsame Anforderungen

- **Handreichungen und Empfehlungen**
  - Geeignetheit und Erforderlichkeit
- **Angemessenheit?**
  - → Maßnahmen unter dem Vorbehalt der technischen Möglichkeit
    - → Z.b. Möglichkeit der beidseitigen Verschlüsselung bei einer Ende-zu-Ende Verschlüsselung
  - → Wirtschaftliche Zumutbarkeit
    - → Verhältnismäßigkeit zwischen Einsatz und Wirkungsgrad der Maßnahme.

Fazit

- **Trotz Handreichungen und Empfehlungen bestehen Unsicherheiten bei der Bestimmung der konkret zu treffenden Vorkehrungen.**
- **Lösungsmöglichkeiten**
  - Etablierung von Best Practice
  - Ggf. mit rechtlicher Wirkung als Genehmigte Verhaltensregel gem. Art. 40 Abs. 2 S. 1 lit. h) DS-GVO

Vielen Dank
für Ihre Aufmerksamkeit

RA Dr. Jan K. Köcher
https://www.dfn-cert.de/
koecher@dfn-cert.de