deutsches forschungsnetz

Gesetzliche Pflichten zur Informations-sicherheit außerhalb Kritischer Infrastrukturen

81. DFN-Betriebstagung| 08.10.2024

Dr. iur. Jan K. Köcher
DFN-CERT Services GmbH

Inhalt

- Welche rechtlichen Rahmenbedingungen gelten für die Prävention vor Cyberangriffen?
- Welche Maßnahmen sind erforderlich?
- Wer ist verantwortlich?

Datenschutz

- Datenschutz-Grundverordnung (DS-GVO)
  - Beschränkt sich auf den Schutz personenbezogener Daten
  - Art. 32 DS-GVO „Sicherheit der Verarbeitung“
  - Abs. 1:“Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche … geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.“
- Dies bedeutet:
  - Geeignete Schutzmaßnahmen: Stand der Technik
  - Angemessenheit: Schutzbedarf im Verhältnis zum Aufwand der Maßnahmen
  - Nachhaltigkeit: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit (Art. 32 Abs. 1 Buchstabe b)
  - Verantwortlichkeit: Die Organisation und damit ihre gesetzlichen Vertreter/-innen

Datenschutz

- Ergänzendes deutsches Recht
  - Grundsatz: Geltungsvorrang der DS-GVO
  - Gesetze in D: Ergänzung + Öffnungsklauseln
    - BDSG: Bundesbehörden, -einrichtungen und private Organisationen
    - Landesdatenschutzgesetze: Behörden und Einrichtungen der Länder
  - Regelungen:
    - BSI-Gesetz: Regelungen zum Datenschutz bei Sicherheitsmaßnahmen für Bundesbehörden und -einrichtungen
    - Vereinzelt in Landesdatenschutzgesetzen ergänzende Regelungen zur zweckändernden Nutzung von Daten zur Informationssicherheit
      - Art. 6 Abs. 1 BayDSG:“Öffentliche Stellen, die personenbezogene Daten verarbeiten dürfen, dürfen diese auch … zur Gewährleistung der Netz- und Informationssicherheit … verarbeiten.“

Informationssicherheit

- **Europäisches Recht**
  - NIS2-Richtlinie
  - Erfordernis der Umsetzung durch nationales Recht bis 17.10.2024
- **Bund: BSI-Gesetz**
  - Richtet sich an Bundesbehörden und Betreiber Kritischer Infrastrukturen
    - BSI als Super-Sicherheitsbehörde
      - Kompetenzen bei der Detektion von Sicherheitslücken und Abwehr von Cyberangriffen
      - Überprüfung von KRITIS-Betreibern
      - Überprüfung von IT-Produkten auf ihre Sicherheit
      - Erarbeitung von Mindeststandards für die Bundesverwaltung
    - Besondere Anforderungen an Betreiber Kritischer Infrastrukturen in § 8a BSI-Gesetz

Informationssicherheit

- Neues BSI-Gesetz zur Umsetzung der NIS-2 Richtlinie
  - Aktueller Stand: Regierungsentwurf vom 24.07.2024
  - Inkrafttreten ursprünglich zum 01.10.2024 geplant
  - Aktuell geplant: März 2025
  - Neuerung ist insbesondere eine erhebliche Ausweitung der zu Maßnahmen verpflichteten Organisationen in:
    - Besonders wichtige Einrichtungen
    - Wichtige Einrichtungen
    - Bundesbehörden werden behandelt wie besonders wichtige Einrichtungen
  - Länder und Kommunen sind nicht direkt reguliert, es erfolgt ein Verweis auf die Zuständigkeit der Länder …

Informationssicherheit

- **Umsetzung NIS-2-Richtlinie**
- **IT-Planungsrat | 03.11.2023 | 42. Sitzung | Beschluss 2023/39**

1. Der IT-Planungsrat beschließt das von der AG Informationssicherheit vorgelegte Identifizierungskonzept der Länder zur Umsetzung der NIS-2-Richtlinie auf regionaler Ebene und bittet die Länder bei der landesrechtlichen Umsetzung der Richtlinie das Identifizierungskonzept einheitlich anzuwenden.
2. Er nimmt den Sachstandsbericht der AG Informationssicherheit zur Kenntnis und bittet die Länder und den Bund, von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen.
3. Ferner bittet der IT-Planungsrat die AG Informationssicherheit ….

Informationssicherheit

- IT-Sicherheitsgesetze Länder
  - Baden-Württemberg: Cyber-Sicherheitsgesetz (CSG BW)
    - Errichtung einer Cybersicherheitsagentur mit weitreichenden Befugnissen
    - Geplant: Rechtsverordnung zur Konkretisierung und flächendeckender Umsetzung einheitlicher Standards
  - Hessen: Hessisches IT-Sicherheitsgesetz (HITSiG)
    - § 3: Pflicht zu angemessenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Informationssicherheit. Maßgeblich ist der Stand der Technik. Außerhalb des kommunalen Bereichs haben sich die Stellen dabei an der IT-Grundschutzmethodik des BSI zu orientieren und ein Informationssicherheitsmanagement umzusetzen.

Informationssicherheit

- IT-Sicherheitsgesetze Länder
  - Niedersachsen: Niedersächsisches Informationssicherheitsgesetz (NDIG)
    - Umsetzung durch Runderlasse geplant
  - Saarland: Informationssicherheitsgesetz Saarland (IT-SiG SL)
    - § 3 verweist bezüglich der Pflichten auf die Anforderungen aus der DS-GVO und dem Saarländischen Datenschutzgesetz. Die Behörden haben angemessene technische und organisatorische Maßnahmen zu treffen und die hierzu erforderlichen Sicherheitskonzepte zu erstellen.
  - Sachsen: Sächsisches Informationssicherheitsgesetz (SächsISichG)
    - § 4 trifft eine vergleichbare Regelung zu Hessen. Das Grundschutz-Kompendium soll aber für alle staatlichen Stellen verbindlich sein. Alle Stellen müssen ein Informationssicherheitsmanagementsystem erstellen und pflegen. Es wird zudem klargestellt, dass grundsätzlich die Leitung der öffentlichen Stelle die Verantwortung trägt.
  - Andere Länder: Mit ähnlichen Vorhaben

Weitere rechtliche Rahmenbedingungen

- Andere Gesetze und rechtliche Verpflichtungen
  - OZG, E-Government Gesetze
    - Regelungen zum elektronischen Zugang zur Verwaltung
    - Allgemeine Regelungen zur Sicherheit, z.B. in § 5 OZG, § 16 EGovG BW
  - Förderbedingungen von Mittelgebern
    - Gegebenenfalls Vorgabe von Zertifizierungen oder Standards
  - Vertragliche Verpflichtungen zur Einhaltung bestimmter Standards zur Informationssicherheit

Fazit

- Es bestehen aus den vorgenannten Rechtsnormen sowohl aus Datenschutz- als auch aus Informationssicherheitsperspektive die folgenden Verpflichtungen:
  - Geeignete Schutzmaßnahmen: Stand der Technik
  - Angemessenheit: Schutzbedarf im Verhältnis zum Aufwand der Maßnahmen
  - Nachhaltigkeit: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit durch Informationssicherheits- und Datenschutzmanagementsysteme
- Verantwortlich für die Umsetzung: Die Organisation und damit ihre gesetzlichen Vertreter oder Leitungen

Haben Sie noch Fragen?

- Kontakt
  - Dr. iur. Jan K. Köcher

E-Mail: koecher@dfn-cert.de
Telefon: 040/ 808077-636
Fax: 040/808077-556

Anschrift:
DFN-CERT Services GmbH
Nagelsweg 41
20097 Hamburg