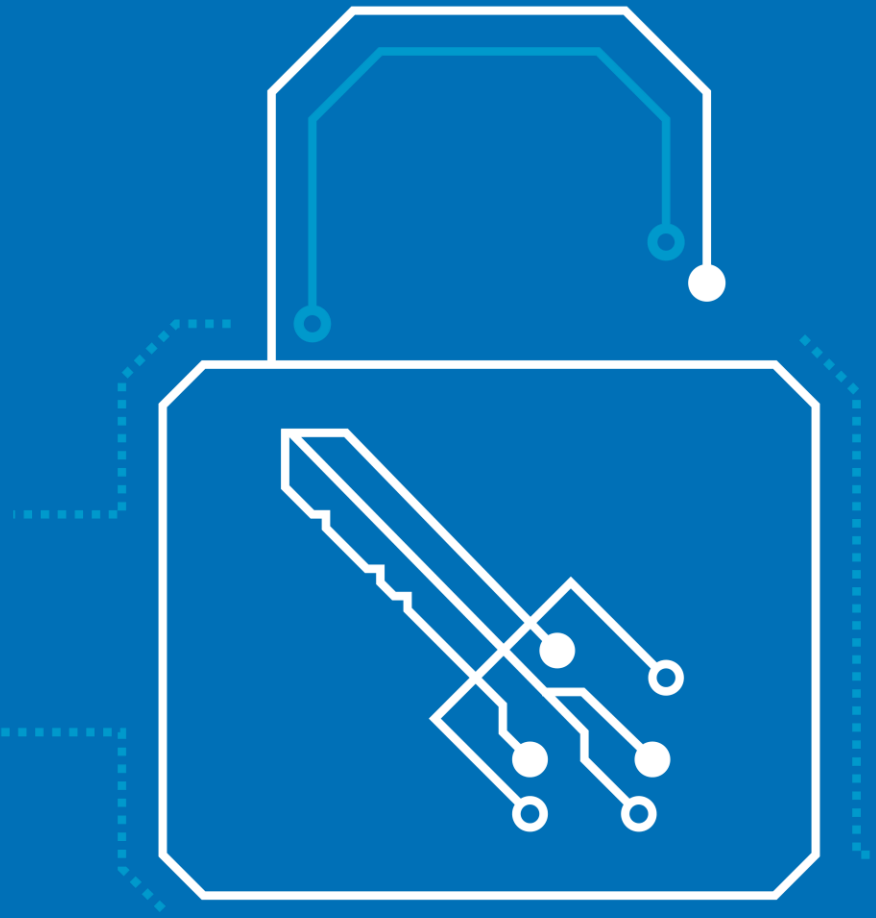
DFN-CERT

Rechtliche Rahmenbedingungen vor und nach Cyberangriffen

Dr. Jan K. Köcher

Das macht uns aus

Das DFN-CERT bietet ein umfangreiches Spektrum an Dienstleistungen rund um das Thema IT-Sicherheit in den Bereichen Netzwerksicherheit, Incident Response, Datenschutz und im Aufbau und Unterhalt skalierbarer und leistungsfähiger Public-Key-Infrastrukturen



Rechtliche Rahmenbedingungen vor Cyberangriffen

Welche rechtlichen Rahmenbedingungen gelten für die Prävention vor Cyberangriffen?

Welche Maßnahmen sind erforderlich?

Wer ist verantwortlich?

Rechtliche Rahmenbedingungen Datenschutz (1)

- 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.”
  - ➢ 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

Rechtliche Rahmenbedingungen Datenschutz (2)

- Ergänzendes deutsches Recht
  - Grundsatz: Geltungsvorrang der DS-GVO
  - Deutsche Gesetze: Ergänzung der DS-GVO und Wahrnehmung von Öffnungsklauseln
    - BDSG: Gilt für Bundesbehörden, Bundeseinrichtungen und private Organisationen
    - Landesdatenschutzgesetze: Behörden und Einrichtungen der Länder

  ➢ Vereinzelt bestehen in den Landesdatenschutzgesetzen ergänzende Regelungen zur zweckändernden Nutzung von Daten für die Informationssicherheit:
  ➢ Art. 6 Abs. 1 BayDSG: “Öffentliche Stellen, die personenbezogene Daten verarbeiten dürfen, dürfen diese auch … zur Gewährleistung der Netz- und Informationssicherheit …. verarbeiten.”

Rechtliche Rahmenbedingungen Informationssicherheit (1)

- Europäisches Recht: NIS2-Richtlinie
- Erfordernis der Umsetzung durch nationales Recht bis Herbst 2024
  - Bund: BSI-Gesetz
  - Richtet sich an Bundesbehörden und Betreiber Kritischer Infrastrukturen
    - ➢ Bundesamt für Sicherheit in der Informationstechnik (BSI) als Superbehörde, u.a.
      - ➢ Kompetenzen bei der Detektion von Sicherheitslücken und Abwehr von Cyberangriffen
      - ➢ KRITIS-Betreiber müssen die Einhaltung der Sicherheit regelmäßig nachweisen und Vorfälle melden
      - ➢ Überprüfung von IT-Produkten auf ihre Sicherheit
      - ➢ Erarbeitung von Mindeststandards für die IT der Bundesverwaltung
    - ➢ Besondere Anforderungen an Betreiber Kritischer Infrastrastrukturen in § 8a BSI-Gesetz
      - ➢ Angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik
      - ➢ Umfasst seit 1.5.2023 auch den Einsatz von Systemen zur Angriffserkennung

Rechtliche Rahmenbedingungen Informationssicherheit (2)

- Bund: Neues BSI-Gesetz zur Umsetzung der NIS-2 Richtlinie
- Aktueller Stand: Referentenentwurf vom 07.05.2024 in der Verbändeanhörung
- Neues BSI-Gesetz soll das bisherige zum 01.10.2024 ersetzen
  - Neuerung zu bisher ist insbesondere eine erhebliche Ausweitung der zu Maßnahmen verpflichteten Organisationen in:
    - Besonders wichtige Einrichtungen (§ 28 BSIG-neu)
    - Wichtige Einrichtungen (§ 28 BSIG-neu)
    - Bundesbehörden werden behandelt wie besonders wichtige Einrichtungen (§ 29 BSIG-neu)
    - Länder und Kommunen sind nicht direkt reguliert, es erfolgt ein Verweis auf die Zuständigkeit der Länder…

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 ….

Rechtliche Rahmenbedingungen Informationssicherheit (3)

- IT-Sicherheitsgesetze Länder:
  - Cyber-Sicherheitsgesetz (CSG BW)
    - Errichtung einer Cybersicherheitsagentur mit weitreichenden Befugnissen
    - Geplant: Rechtsverordnung zur Konkretisierung und flächendeckender Umsetzung einheitlicher Standards
  - 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.

Rechtliche Rahmenbedingungen Informationssicherheit (4)

- Niedersächsisches Informationssicherheitsgesetz (NDIG)
- 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.
- 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: Sind noch nicht soweit

Weitere Rechtliche Rahmenbedingungen

- OZG, E-Government Gesetze
  - Regeln den elektronischen Zugang zur Verwaltung
  - Diese Möglichkeiten fließen über die Angemessenheit in die erforderlichen Sicherheitsmaßnahmen der öffentlichen Stellen ein.
  - Allgemeime Regelung zur Sicherheit z.B. in § 5 OZG, § 16 EGovG BW

- Förderbedingungen von Mittelgebern
  - Ggf. Vorgabe von 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

  - Verantwortlichkeit zur Umsetzung: Die Organisation und damit ihre gesetzlichen Vertreter oder Leitungen

Exkurs: 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 (Begründung zum 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.

Rechtliche Rahmenbedingungen nach Cyberangriffen

Welche rechtlichen Pflichten gelten nach Cyberangriffen?

Rechtliche Pflichten
Datenschutz (1)

- Datenschutz-Grundverordnung (DS-GVO)
  - Beschränkt sich auf den Schutz personenbezogener Daten
  - Art. 33 DS-GVO: Meldepflicht an die zuständige Aufsichtsbehörde
  - Innerhalb von 72 Stunden nach Bekanntwerden des Datenschutzvorfalls
  - Auftragsverarbeiter haben einen Vorfall unverzüglich an den Verantwortlichen zu melden
  - Ausnahmsweise keine Pflicht wenn die Verletzung voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten natürlicher Personen führt.
  - ➢ Inhalt der Meldepflicht:
    - ➢ Beschreibung der Art der Verletzung, Datenkategorien, ungefähre Zahl der Betroffenen, ungefähre Zahl der betroffenen Datensätze
    - ➢ Name und Kontaktdaten des/der DSB
    - ➢ Beschreibung der wahrscheinlichen Folgen
    - ➢ Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen

Rechtliche Pflichten
Datenschutz (2)

- Art. 34 DS-GVO: Meldepflicht an betroffene Personen
- Nur wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen hat
- Die Benachrichtigung ist nicht erforderlich:
  - Der Verantwortliche hat geeignete technische und organisatorische Vorkehrungen getroffen (z.B. Verschlüsselung)
  - Sicherstellung durch nachfolgende Maßnahmen
  - Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall muss eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen.
- Inhalt der Meldung: In einfacher und verständlicher Sprache:
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der ergriffenen Maßnahmen

Rechtliche Pflichten Informationssicherheit (1)

- BSI-Gesetz
  - Derzeit nur KRITIS-Betreiber

- IT-Sicherheitsgesetze der Länder
- § 16 SächsISichG:
- Es besteht eine Meldepflicht bei Sicherheitsvorfällen an das Sicherheitsnotfallteam. Eine unverzügliche Meldung hat zu erfolgen:
  - ➢ Bei erheblichen Beeinträchtigungen
  - ➢ Potentiell behördenübergreifende erhebliche Beeinträchtigungen
  - ➢ Die Meldepflicht umfasst auch die statistischen Angaben und Protokolldaten von Schutzsystemen

Rechtliche Pflichten Informationssicherheit (2)

- Hessen, Saarland
- § 17 HITSiG, § 9 IT-SiG SL : Pflicht zur Information Betroffener wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist
- § 18 HITSiG, § 3 Abs. 2 IT-SiG SL : Unverzügliche Meldepflicht an das Zentrum für Informationssicherheit, wenn Informationen bekannt werden, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind

Vielen Dank für Ihre Aufmerksamkeit!