Rechtliche Aspekte im Forschungs-Daten-Management

Informationssicherheit – Gesetze, Standards, Richtlinien der Universität

Dr. Holger Beck
Informationssicherheitsbeauftragter der Georg-August-Universität Göttingen
IT-Sicherheitsbeauftragter der GWDG

Informationssicherheit

=

Sicherheit von Informationen

Was heißt das?

Erklärung über Informationssicherheitsziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Vertraulichkeit

Gewährleistung des Zugangs zu und Zugriffs auf Informationen nur für Berechtigte

Integrität

Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden

Verfügbarkeit

Gewährleistung des bedarfsorientierten Zugriffs auf Informationen für Berechtigte

Häufig auch mit englischen Bezeichnungen

- Confidentiality
- Integrity
- Availability

Abgekürzt: CIA

Manchmal auch zusätzliche spezielle Ziele:

- Authentizität
- Nachvollziehbarkeit
- Nicht-Abstreitbarkeit
- …

Anmerkung: Teils abweichende Ziele im Datenschutz

- Datensparsamkeit
- Transparenz
- Korrektur
- Löschen
- Nichtverkettbarkeit
- …

IT-Sicherheit vs. Informationssicherheit

- Manchmal als Synonym betrachtet
- oder stärker Perspektive von der Technik ausgehend bei IT-Sicherheit (Bottom-Up vs. Top-Down)

Gesetze zur Informationssicherheit

- **IT-Sicherheitsgesetz**
  - Enthält Regelungen für
    - BSI (Bundesamt für Sicherheit in der Informationstechnologie)
    - Kritische Infrastrukturen
      - Definition
      - Pflichten
      - Anforderungen
- **Nicht relevant für Forschungs-Daten-Management**
  - Aber für die Krankenversorgung in der Universitätsmedizin Göttingen (UMG)

Gesetze zur Informationssicherheit

- KonTraG
  - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
  - Nicht direkt Informationssicherheit, aber über Betrachtung von Risiken indirekt
- Strafgesetzbuch
  - Strafen für Computersabotage usw.
- Telekommunikationsgesetz und Telemediengesetz
  - Für Betreiber von Telekommunikationsdiensten (Netze, E-Mail-Dienste) oder Telemediendiensten (z.B. Webserver)
- Nicht direkt für Forschungs-Daten-Management

Gesetze zur Informationssicherheit

- EU-DSGVO und Bundes- und Landesdatenschutzgesetze
- Relevant für Forschungs-Daten-Management
  - soweit personenbezogene Daten verarbeitet werden,
  - aber in eigenen Vorträgen schon behandelt.

Nochmal IT-Sicherheitsgesetz

- Festlegung von kritischen Infrastrukturen (KRITIS) im §2 BSI-Gesetz (BSIG)
  - „(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die
    - 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, **Gesundheit**, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
    - 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Nochmal IT-Sicherheitsgesetz

- Pflichten für Betreiber kritischer Infrastrukturen nach BSIG
  - Einrichtung einer Kontaktstelle (§8b Abs. 3)
  - Meldepflichten bei Störungen (§8b Abs. 4)
  - Sicherheit in der Informationstechnik (§8a)
    - „(1) Betreiber Kritischer Infrastrukturen sind verpflichtet … angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. …“
    - (3) Nachweispflicht zu (1) alle 2 Jahre

Nochmal IT-Sicherheitsgesetz

- Festlegung von Kritischen Infrastrukturen in Kritis-Verordnung
  - für Sektor Gesundheit in kritische Dienstleistungen:
    - die stationäre medizinische Versorgung,
    - die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind,
    - die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper,
    - die Laboratoriumsdiagnostik;
  - und abhängig von Umfang (z.B. mehr als 30.000 Fälle pro Jahr für stationäre medizinische Versorgung)

Standards in der Informationssicherheit

- Grundlage für (meist freiwillige) Zertifizierungen,
- Orientierungshilfen (Stand der Technik)

Standards in der Informationssicherheit

- ISO 2700x
- IT-Grundschutz des BSI
- Branchenspezifische Sicherheitsstandards (B3S) nach BSIG
- ISIS12 und spezielle Standards in Industriezweigen o.ä.

ISO 2700x

- Familie von Normen,
- Internationaler Standard für Informationsmanagementsysteme
- „Hauptteil“ ISO 27001
  - Titel: “Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen”
  - Allgemeine Anforderungen in 10 Kapiteln und Anhang aus 35 Seiten
  - Normativer Anhang mit 114 Maßnahmen (Controls)
  - Leitfaden für Informationssicherheitsmaßnahmen in ISO27002
    - Erläuterung zu den 114 Maßnahmen auf 112 Seiten
- Relativ allgemeine Anforderung, wenig Detailvorgaben
- Zertifizierung nach ISO 27001 international anerkannt

IT-Grundschutz

- Deutscher Standard
- Zertifizierung möglich
- Standards des BSI
  - BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS) (48 Seiten)
  - BSI-Standard 200-2 IT-Grundschutz-Methodik (180 Seiten)
  - BSI-Standard 200-3 Risikomanagement (54 Seiten)
- IT-Grundschutzkompendium (810 Seiten)
- IT-Grundschutzprofile für spezielle Anwendungen
  - IT-Grundschutzprofile für Hochschulen
    - Entwickelt von ZKI, Allianz für Cybersicherheit/BSI
    - Fokus aber auf Verwaltungstätigkeiten/Prozesse im Rahmen der Lehre

IT-Grundschutzkompendium

- Elementare Gefährdungen
- Bausteine in 10 Bereichen
  - Teils mehrstufig unterteilt
  - In den Bausteinen (z.B. Organisation, Personal, Behandlung von Sicherheitvorfällen, Webanwendungen)
    - Beschreibung
    - Gefährdungslage
    - Anforderungen (früher Maßnahmenkataloge) in Kategorien
      - Basis-Anforderungen
      - Standard-Anforderungen
      - Anforderungen bei erhöhtem Schutzbedarf
- Sehr detailliert, daher auch als Orientierung zum Stand der Technik geeignet.

Branchenspezifischer Sicherheitstandard (B3S)

- Option im IT-Sicherheitsgesetz für KRITIS-Branchen (§8a Abs. 2 BSIG)
  - Branchen können Standards vorschlagen
  - BSI stellt auf Antrag Eignung fest
  - B3S kann dann als Prüfgrundlage für die Erstellung der geforderten Nachweise dienen.
- B3S für Branche medizinische Versorgung
  - Von DKG (Deutsche Krankenhausgesellschaft) unter mitwirkung des UPKRITIS-Branchenarbeitskreises (BAK) erstellt
  - Eignungsfeststellung 2019
  - Von UMG als Prüfgrundlage genutzt
  - 88 Seiten, u.a. 168 Anforderungen an Maßnahmen und 37 an Risikomanagement

Informationssicherheitsrichtlinie der Universität

- Seit dem 25.01.2020 ist die (neue) Richtlinie zur Informationssicherheit der Universität in Kraft
  - Veröffentlicht in den Amtlichen Mitteilungen (https://uni-goettingen.de/de/619701.html)
  - Siehe auch https://it-sicherheit.uni-goettingen.de
- Struktur (Auszug)
  - Grundsätze
  - Organisatorische Festlegungen (Rollen und Aufgaben)
  - Inhaltliche Festlegungen
  - Anlage Maßnahmenkatalog für den IT-Grundschutz
    - Maßnahmen für Anwender (22 Maßnahmen)
    - Maßnahmen für IT-Personal (zusätzliche 43 Maßnahmen)

Abschnitte, Paragraphen, Anlagen

Abschnitt I: Grundsätze
- § 1 Gegenstand und Geltungsbereich
- § 2 Rahmenbedingungen
- § 3 Sicherheitsziele
- § 4 Informationssicherheitsprozess

Abschnitt II: Organisatorische Festlegungen
- § 5 Präsidium und Vorstand
- § 6 IT-Steuerungsgruppe und CIO
- § 7 IT-Dienstleister
- § 8 Zuständige Leitung
- § 9 Informationssicherheitskoordinatorinnen und Informationssicherheitskoordinatoren (ISK)
- § 10 Fachverantwortliche
- § 11 Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB)
- § 12 Informationssicherheitsmanagerinnen oder Informationssicherheitsmanager (ISM)
- § 13 Datenschutz- und Informationssicherheits-Beirat (DIB)

Abschnitt III: Inhaltliche Festlegungen
- § 14 Maßnahmenkatalog für den IT-Grundschutz
- § 15 Zusätzliche Maßnahmen
- § 16 Umgang mit Informationssicherheitsvorfällen
- § 17 Gefahrenintervention

Abschnitt IV: Schlussbestimmungen
- Anlage 1 Festlegung der zuständigen Leitung der jeweiligen Einheit
- Anlage 2 Maßnahmenkatalog für den IT-Grundschutz
- Anlage 3 Glossar

Regeln – was ist wirklich wichtig

- Die Richtlinie wurde entsprechend den Bedürfnissen der Juristen verfasst (mit §§ usw.)
  - erscheint vielleicht manchmal also etwas bürokratisch und formalistisch,
  - für den Anwender enthält aber der Teil „Maßnahmen für Anwender“ die wichtigsten und in der Praxis relevanten Regeln (in 22 Maßnahmen)

- Im Weiteren
  - Kurzer Blick auf die Maßnahmen für Anwender
  - Mehr zu einer Auswahl von Maßnahmen (bzw. den praktischen Aspekten)

Maßnahmen für IT-Anwender

… Überblick

A.1 Anwenderqualifizierung
A.2 Meldung von IT-Problemen
A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen
A.4 Kontrollierter Softwareeinsatz
A.5 Schutz vor Viren und anderer Schadsoftware
A.6 Zutritts-, Zugangs- und Zugriffskontrolle
A.7 Sperren und ausschalten
A.8 Sicherung von Notebooks, mobilen Speichermedien, Smartphones
A.9 Personenbezogene Nutzerkonten
A.10 Gebrauch von Passwörtern
A.11 Zugriffsrechte
A.12 Netzzugänge
A.13 Telearbeit
A.14 Sichere Netzwerknutzung - Allgemeine Anforderungen
A.15 Sichere Netzwerknutzung - E-Mail
A.16 Datenspeicherung
A.17 Nutzung externer Dienste
A.18 Nutzung privater Hard- und Software
A.19 Datensicherung und Archivierung
A.20 Umgang mit Datenträgern
A.21 Löschen und Entsorgung von Datenträgern
A.22 Sichere Entsorgung vertraulicher Papiere

A. 16 Datenspeicherung

Verantwortlich für Initiierung:	Fachverantwortliche
Verantwortlich für Umsetzung:	IT-Personal

(1) Dienstliche Daten sind grundsätzlich innerhalb der IT-Systeme der Stiftungsuniversität Göttingen (einschließlich der von der GWDG für die Stiftungsuniversität betriebenen IT-Systeme) zu speichern.

(2) Dabei sind die Möglichkeiten der Speicherung auf zentralen Servern zu nutzen.

(3) Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatzrechners oder anderer lokaler Speichermedien ist nur zulässig, wenn das spezifische Informationssicherheitskonzept für den jeweiligen Datenbestand dies zulässt und die darin festgelegten Sicherheitsmaßnahmen getroffen wurden.

(4) Die Speicherung (und Verarbeitung) dienstlicher Daten außerhalb der IT-Systeme der Stiftungsuniversität Göttingen (z.B. auf Cloud-Diensten oder privaten Geräten) ist nur zulässig, wenn dies dienstlich erforderlich ist und das spezifische Informationssicherheitskonzept für den jeweiligen Datenbestand diese Speicherung zulässt. Bei einer externen Speicherung ist eine dem Schutzbedarf angemessene Sicherung der Daten gegen Verlust der Daten, der Vertraulichkeit und der Integrität der Daten zu gewährleisten. Möglichkeiten zur Rückholung der Daten vom und deren Löschung auf dem externen Speicher müssen sichergestellt sein.

(5) Die Speicherung schutzwürdiger Daten außerhalb der IT-Systeme der Stiftungsuniversität Göttingen ist nur in den Staaten des europäischen Wirtschaftsraums und sicheren Drittstaaten entsprechend dem Datenschutzrecht zulässig.

A.22 Datensicherung und Archivierung

Verantwortlich für Initiierung:	Fachverantwortliche
Verantwortlich für Umsetzung:	IT-Personal, Fachverantwortliche

(1) Daten müssen vor Verlust durch Fehlbedienung, technische Störungen o. ä. geschützt werden. Dazu müssen regelmäßig Datensicherungen (Anlegen von Kopien der Daten auf getrennten Speichersystemen) durchgeführt werden.

(2) Ist die Speicherung auf zentralen Servern mit geregelter Datensicherung nicht möglich, sind die jeweiligen Fachverantwortlichen für die Sicherung der Daten selbst verantwortlich.

(3) Bei zentraler Datensicherung haben sich die Fachverantwortlichen über die jeweils geltenden Bestimmungen zu Rhythmus und Verfahrensweise für die Datensicherung zu informieren.

(4) Von der Datensicherung zum Schutz vor Verlust ist die zur Umsetzung der „Ordnung der Georg-August-Universität Göttingen zur Sicherung guter wissenschaftlicher Praxis“ nötige Langzeitarchivierung wissenschaftlicher Daten zu unterscheiden. Diese ist von den Fachverantwortlichen sicherzustellen.

Maßnahmen für IT-Personal

- Auswahl mit Blick auf Datenmanagement
  - I.39 Organisation der Datensicherung
  - I.40 Anwenderinformation zur Datensicherung
  - I.41 Verifizierung der Datensicherung
  - I.42 Löschen und Entsorgen von Datenträgern
  - I.43 Sichere Entsorgung vertraulicher Unterlagen

Danke

Fragen?

Agenda

- Rechtliche Aspekte mit Blick auf Informationssicherheit
  - Gesetzliche Regelungen
    - für Aktiengesellschaften,
    - kritische Infrastrukturen (auch stationäre medizinische Versorgung in der UMG)
  - aber für Forschungsdaten an der Universität
    - keine konkreten gesetzlichen Vorgaben (mit Blick auf Informationssicherheit)
  - Standards der Informationssicherheit
    - Grundlage für (freiwillige) Zertifizierungen,
    - Orientierungshilfen (Stand der Technik)
  - Regeln der Universität
    - insbesondere die Informationssicherheitsrichtlinie