Informationssicherheit und Datenschutz an Hochschulen

Leistungen des DFN-CERT

Informationssicherheit als strategische Aufgabe der Hochschulleitung, Workshop der HRK in Berlin am 25. und 26. November 2019

Dr. Jan K. Köcher
koecher@dfn-cert.de

Kurzvorstellung DFN-CERT

- **DFN-CERT Services GmbH**
  - 1993 bis 1999 als Projekt an der Uni Hamburg gestartet
  - Entwicklung zum hochspezialisierten Dienstleister für Informationssicherheit und Datenschutz im DFN
  - Primär betreute Klientel: Anwender des DFN-Vereins
- **Arbeitsschwerpunkte / Teams**
  - Incident Response
  - PKI, Infrastruktur Services
  - Projekte und Entwicklung
  - ***Consulting, Analyse und Training***
- **Veranstaltungen**
  - Organisation jährlicher DFN-Konferenzen:
    - *'Sicherheit in vernetzten Systemen'*
    - *'Datenschutz'*
  - Tutorien, Workshops und Schulungen

Lage an den Einrichtungen

- **Bedeutung der Informationssicherheit ist noch nicht überall angekommen**
- **Informationssicherheitsmanagement ist**
  - Teuer
    - Budget wird woanders gebraucht, kein Personal!
  - Sinnlos
    - Hochschulen werden nicht angegriffen!
    - Das Rechenzentrum macht das schon!
    - Schafft keinen Mehrwert, eh nur – zuviel - Papier!
  - Wirkungslos
    - Freiheit von Forschung und Lehre!

Herausforderungen

- **Defizite bei den betreuten Einrichtungen**
  - Organisatorischer Überbau / Verantwortung der Leitungsebene
  - Ansprechpartner für Informationssicherheit
  - Erkennung und Behandlung von Sicherheitsvorfällen
    - Meldepflichten aus der DS-GVO!
  - Asset-, Schwachstellen- und Änderungs-Management
  - Integration in Geschäftsprozesse
  - Sensibilisierung und Notfallplanung

Gegen,- Neben- oder Miteinander?

- **Beispiel: Ransomware**
  - Technische Maßnahmen allein nicht ausreichend!
  - Daher ist nur eine Mischung aus organisatorischen und technischen Maßnahmen zielführend!
    - Awareness / Sensibilisierung
    - Backup / Datensicherung
    - Meldestelle für Vorfälle
    - Informationsportal
    - Notfallpläne?

- **Gesamtheitliche Informationssicherheit ist nur Miteinander zu erreichen!**

Dienstleistungsportfolio

- **Informationssicherheit und Datenschutz**
  - Bestandsaufnahme
  - Entwicklung einer passenden Sicherheitsstrategie
  - Durchführung von Risikoanalysen
  - Aufbau eines Informationssicherheitsmanagement-systems (ISMS)
  - Erstellung und Umsetzung von Sicherheits-konzepten
  - Audit und Zertifizierung
  - Auditierung und Beratung zum Datenschutz

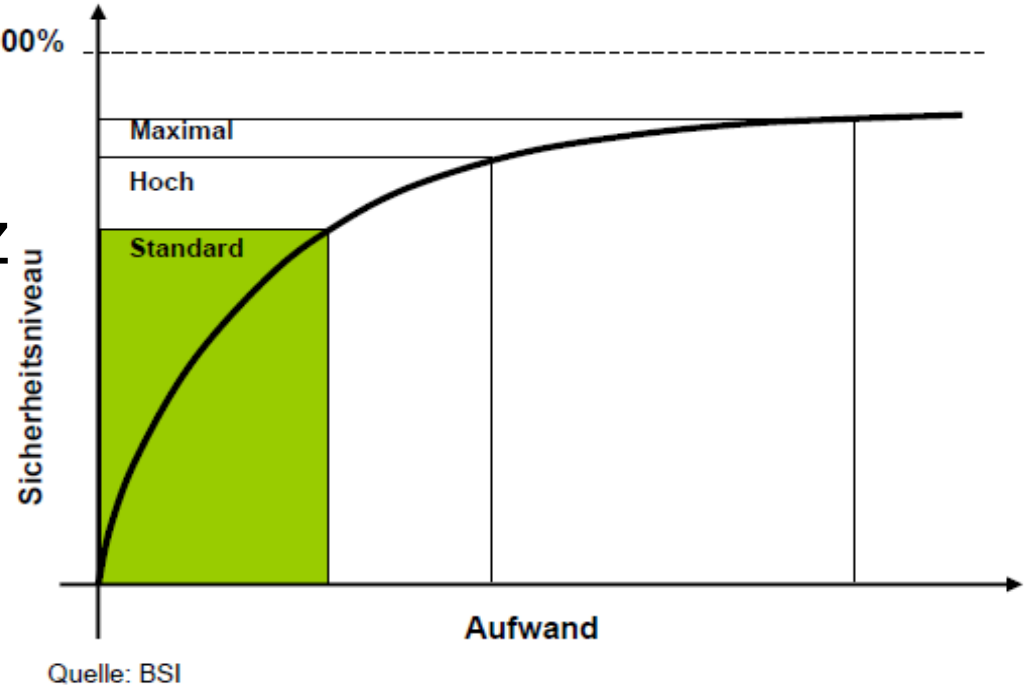
Bestandsaufnahme

- **Unterstützung bei der Beantwortung der Fragestellung: 'Wo stehen wir?'**
  - Leistungsumfang, von
    - der Dokumentenprüfung,
    - über Begehungen und Interviews,
    - der Ausführung von Penetrationstests,
    - bis zur Durchführung von Audits.
  - Ergebnisse bilden eine Basis für die weitere Planung, u.a.: für die Abschätzung der
    - Aufwände
    - Zeiträume
    - Investitionen

Sicherheitsstrategien

- **Hilfestellung bei der Fragestellung:**
  - 'Wo wollen wir hin?', bzw.
  - 'Was müssen wir umsetzen?'
  - Mögliche Anforderungen:
    - Vermeidung interner Sicherheitsvorfälle
    - Compliance
    - Datenschutz
    - IT-Sicherheitsgesetz
    - ...

→ **Entwicklung der Sicherheitsstrategie**



Quelle: BSI

Risikoanalyse

- **Risikoanalyse mit OCTAVE**

  Operationally Critical Threat, Asset and Vulnerability Evaluation

  - Entwickelt vom CERT/CC der Carnegie Mellon University
  - Schwerpunkt: wertebezogene Analyse der Risiken und Sicherheitsprozesse
  - Übersetzung auf Deutsch, Anpassung an ISO 27001 und IT-Grundschutz
  - Unterstützung der Anwender durch Arbeitsblätter, Fragen, Checklisten und Tipps

Beratung der Hochschulleitung

- Unterstützung bei der Etablierung eines Informationssicherheitsmanagementsystems (ISMS)
- Schulung des Informationssicherheitsbeauftragten (auch BIS, ISB oder CISO) mit Abschlussprüfung und Zertifikat
- Unterstützung bei der Erstellung von übergeordneten Dokumenten zur Informationssicherheit, z.B.:
  - Leitlinie
  - Sicherheitsordnung
  - Sicherheitsrichtlinien

Sicherheitskonzepte

- **Leistungen des DFN-CERT**
  - Erstellung von Sicherheitskonzepten anhand von Zielvorgaben, z.B. nach
    - IT-Grundschutz / ISO 27001,
    - Vorgaben des Datenschutzes (technische und organisatorische Maßnahmen - TOMs),
    - 'Best Practices'
    - oder sonstiger Anforderungen.
  - Begleitung bei der Umsetzung
  - Audit und Zertifizierung

Datenschutz

Beratung zum Datenschutz

- Bestandsaufnahme
- datenschutzgerechte Modellierung von Verfahren und Prozessen
- Unterstützung beim Aufbau eines Datenschutz-managements (DSMS) entsprechend der Nachweispflichten aus der DS-GVO
- Unterstützung bei Datenschutz-Folgeabschätzungen
- Coaching von Datenschutzbeauftragten und -manager*innen

- Gutachten zu Fragestellungen des Datenschutzes
- Schulungen

Unsere Grundlagen

- **Beratungsleistungen und Empfehlungen orientieren sich an**
  - den 'Best Practices' aus dem Forschungs- und Hochschulbereich,
  - dem IT-Grundschutz des BSI,
  - den ISO Normen 2700x,
  - den Publikationen der Zentren für Kommunikation und Informationsverarbeitung (ZKI) in Lehre und Forschung e.V.,
  - und natürlich aus unseren langjährigen Erfahrungen.

Expertise

- **Zertifizierungen, Akkreditierungen und Prüfungen der CAT-Mitarbeiter:**
  - Akkreditierter ISO 27001 Lead Auditor
  - Zertifizierter ISO 27001-Auditor auf Basis von IT-Grundschutz (BSI)
  - Zertifizierter Datenschutzbeauftragter (TÜV)
  - Zertifizierter Datenschutzauditor (TÜV)
  - Betrieblicher Datenschutzbeauftragter (GDDcert.)
  - Certified Information Systems Security Professionals (CISSP)

DFN CERT®

Vielen Dank
für Ihre Aufmerksamkeit!

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