Umsetzung von Informationssicherheits-prozessen bei DFN-Teilnehmern

Dr. Christian Paulsen
DFN-CERT Services GmbH
paulsen@dfn-cert.de

Kurzvorstellung

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

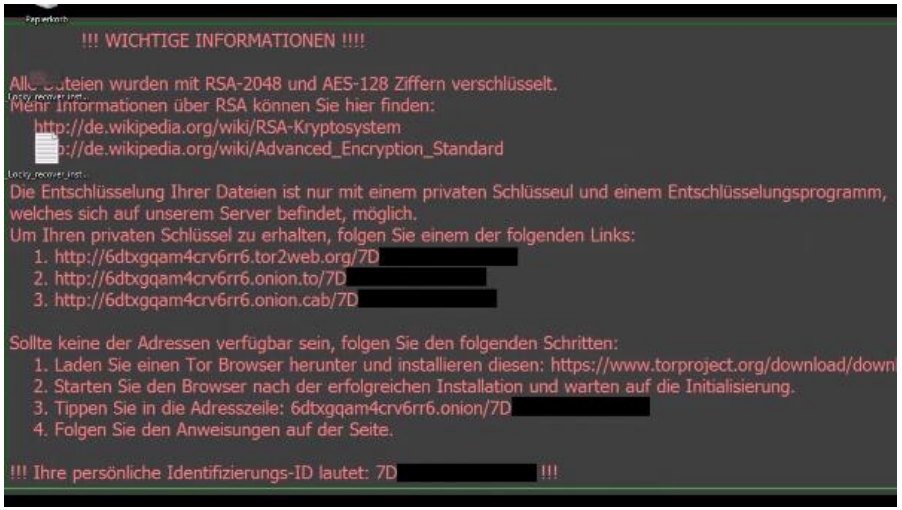
IT-Sicherheit vs. Informationssicherheit

- **IT-Sicherheit ist nur eine Teilmenge von Informationssicherheit**
  - *Alle* Informationen müssen geschützt werden, d.h. auch Know-How und Papierdokumente
  - Organisatorische und technische Sicherheitsmaßnahmen sind gleichwertig:
    - Das beste Firewallkonzept ist ohne Zutrittskontrollmaßnahmen hinfällig
    - Der (ungeschulte) Benutzer als schwächstes Glied der Sicherheitskette

Aufgaben & Ziele eines ISMS

- Festlegung von Sicherheitszielen
- Ermittlung und Bewertung von Informationssicherheitsrisiken
- Auswahl geeigneter Sicherheitsmaßnahmen
- Überwachung der Einführung und des laufenden Betriebs der Maßnahmen
- Kontinuierliche Verbesserung
- Förderung des Sicherheitsbewusstseins innerhalb der Organisation
- Erkennung und Reaktion auf Vorfälle

Beispiel: Ransomware „Locky“



Bildquelle: Heise.de

- Technische Maßnahmen alleine nicht wirksam
- Daher Mischung aus technisch-organisatorischen Maßnahmen erforderlich, u.a.:
  - Regelmäßige Awareness-Schulungen
  - Ein adäquates Backupkonzept
  - Anlaufstelle für die Meldung von Vorfällen
  - Informationsportal für Informationssicherheit
  - Notfallpläne

Lage an Hochschulen

- Bedeutung der Informationssicherheit (noch) nicht überall angekommen
- Sehr heterogene Strukturen, abhängig von personellen und finanziellen Gegebenheiten
- In der Regel historisch gewachsene (IT-)Strukturen
- Abhängigkeit von Know-How und Engagement der Mitarbeiter
- Hohe Fluktuation beim Personal
- Teilweise geringe Akzeptanz für Sicherheitsmanagement

ISMS an Hochschulen?

- **Teuer:**
  - Budget wird woanders gebraucht!
  - Personal ist sowieso nicht da!
- **Sinnlos:**
  - Hochschulen werden nicht angegriffen!
  - Das Rechenzentrum macht das schon!
  - Schafft keinen Mehrwert – keiner braucht das!
  - Ist eh nur - zuviel - Papier!
- **Wirkungslos:**
  - Freiheit von Forschung und Lehre!

Gründe für ISMS (1)

- **Mittelfristig werden Kosten gesenkt**

- **Sicherheitsvorfälle sind teuer**
  - Eingeschränkte Nutzbarkeit
  - Verlorene Zeit
  - Sanktionierung und Haftung
  - Wiederherstellungskosten
  - Rufschäden
  - …

Gründe für ISMS (2)

- **IS-Management schafft Klarheit**
  - Klare Zuständigkeiten
  - Verteilte Verantwortung
  - Vertretungsregelungen
  - Kommunikationsaufwand sinkt
  - Einarbeitungszeit für neues Personal sinkt
  - Benutzer wissen, was wann zu tun ist

Gründe für ISMS (3)

- **Abhängigkeit von IT-Systemen nimmt zu**
  - Aufsichtsbehörden (z.B. Rechnungshöfe) verlangen Sicherheitskonzepte
  - Datenschutzgesetze verlangen technisch-organisatorische Maßnahmen
  - Vorteile bei Drittmittelvergaben und Hochschulrankings
  - Grundsatzpapier der Allianz der Wissenschaftsorganisationen

Gründe für ISMS (4)

Allianz der Wissenschaftsorganisationen

Alexander von Humboldt-Stiftung
Deutsche Forschungsgemeinschaft
Fraunhofer-Gesellschaft
Hochschulrektorenkonferenz
Leibniz-Gemeinschaft
Deutsche Akademie der Naturforscher Leopoldina – Nationale Akademie der Wissenschaften
Deutscher Akademischer Austauschdienst
Helmholtz-Gemeinschaft
Max-Planck-Gesellschaft
Wissenschaftsrat

Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen

Für die Arbeit an wissenschaftlichen Einrichtungen sind Dienstleistungen der Informations- und Kommunikationstechnik (IKT bzw. IT) von zunehmender Bedeutung. Damit nimmt auch die Abhängigkeit von der Funktionstüchtigkeit einer IKT stetig zu. Gleichzeitig bedarf es für hochwertiges wissenschaftliches Arbeiten in Forschung und Lehre einer angemessenen Informations- und IT-Sicherheit. Es ist daher unerlässlich, umfassende Schutzmaßnahmen zu ergreifen. Hierfür sollte nach Auffassung der in der Allianz der Wissenschaftsorganisationen verbundenen Einrichtungen jede wissenschaftliche Einrichtung eine grundlegenden IT-Sicherheitsstrategie formulieren, verabschieden und auf Leitungsebene verankern, die die Basis für ein IT-Sicherheitskonzept und daraus folgende Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik darstellt.

Gründe für ISMS (5)

- **Hochschulen sind lohnendes Angriffsziel**

- **Beispiele für schützenswerte Daten**
  - Forschungsdaten
  - Patentdaten
  - Projektergebnisse
  - Prüfungsergebnisse
  - Personaldaten
  - Studierendendaten

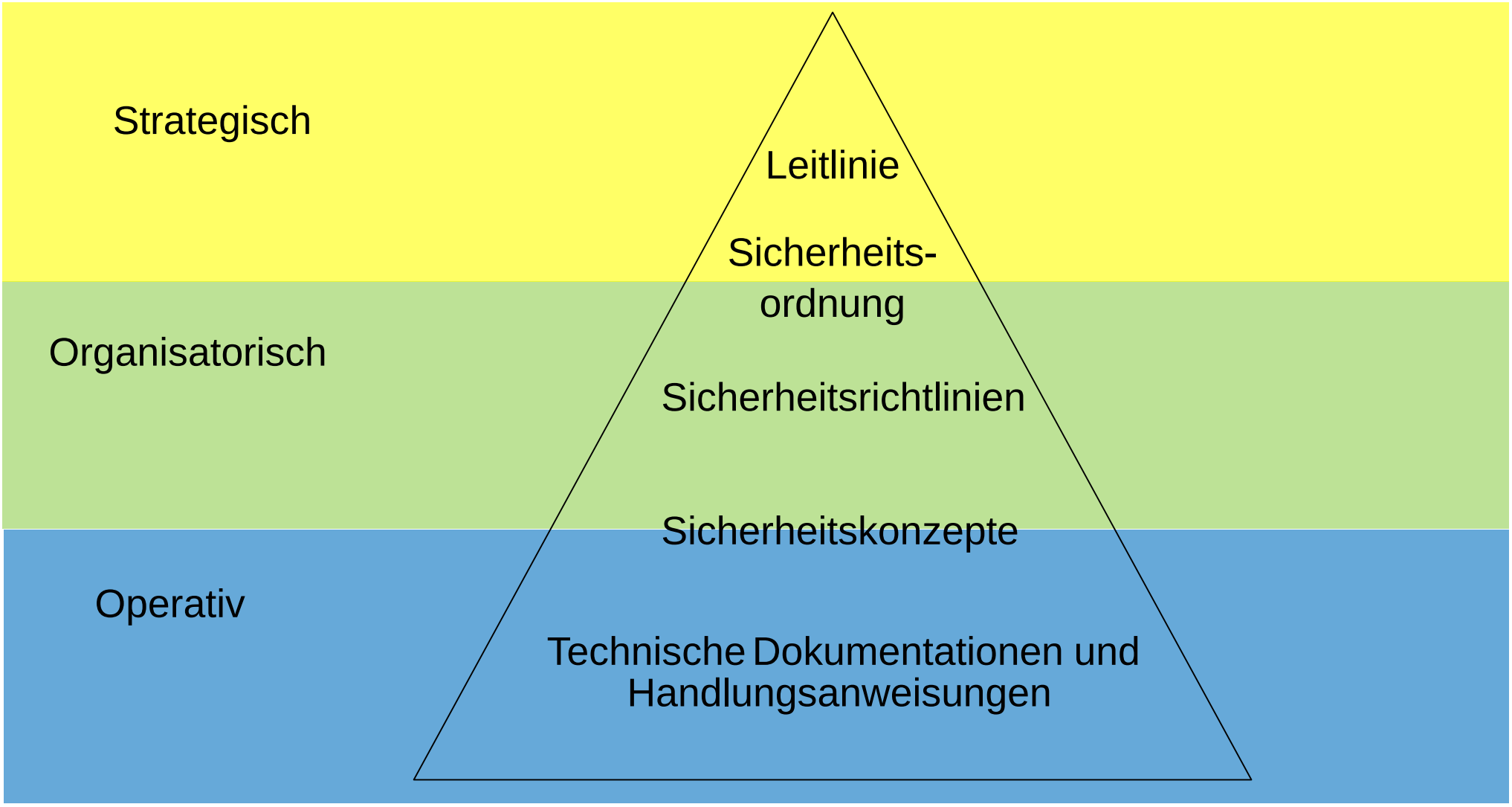
- **Angriffe finden permanent statt**

Gründe für ISMS (6)

- **Sicherheit ist Leitungsaufgabe**
  - Hochschulen wurden 2006 in die „Hochschulfreiheit“ entlassen
  - Verantwortung für Sicherheit liegt wie in der freien Wirtschaft bei der HS-Leitung

- **Rechenzentren müssen entlastet werden**
  - Immer mehr Systeme zu betreuen
  - Erhöhte Nutzeranforderungen & Komplexität
  - Parallel dazu soll hoher Sicherheitsstandard und gute Performanz geliefert werden

Aufbau eines ISMS



Fazit

- **ISMS an Hochschulen ist machbar**
  - Sicherheitsziele definieren / Risikoanalysen durchführen
  - Stabsstellen und dezentrale Ansprechpartner etablieren
  - Regelmäßig Awareness-Kampagnen und Schulungen durchführen
  - Schrittweiser Aufbau einer hierarchischen Managementstruktur
  - Verbindliche Richtlinien und Konzepte
  - Rechte UND Pflichten von Organisationseinheiten definieren
  - Sanktionierungsmöglichkeiten schaffen

Vielen Dank
für die Aufmerksamkeit

Dr. Christian Paulsen
https://www.dfn-cert.de/
paulsen@dfn-cert.de