IT BRAUCHT SICHERHEIT

Datenschutz und IT-Sicherheit an der UniBi

1. Dezember 2009

Ines Meyer
Michael Sundermeyer

Datenschutz

- Datenschutz hat Verfassungsrang
  - „Recht auf informationelle Selbstbestimmung
- Datenschutzgesetz Nordrhein-Westfalen
  - viele bereichsspezifische Regelungen in anderen Gesetzen (z.B. TKG, Meldegesetz, SGB etc.)
- Schutz personenbezogener Daten
  - nur bei Verarbeitung personenbezogener Daten Anwendung datenschutzrechtlicher Vorschriften

Datenschutzbeauftragte

- Seit 2000 gesetzliche Einführung eines behördlichen Datenschutzbeauftragten
  - Unterstützung der Einrichtung bei der Sicherstellung des Datenschutzes
  - Beratung bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten
  - Überwachung bestehender oder neuer Verfahren und der Einhaltung datenschutzrechtlicher
  - Schulungen
  - Durchführung der Vorabkontrolle
  - Führung Verfahrensverzeichnis

Zulässigkeit der Datenverarbeitung

- „Verbot mit Erlaubnisvorbehalt“
- Datenverarbeitung muss **gesetzlich erlaubt** oder von der **Einwilligung** des Betroffenen umfasst sein

Datenschutz-Grundsätze

1. Grundsatz der Zweckbindung
2. Grundsatz der Datensparsamkeit
3. Grundsatz der Datenvermeidung
4. Verhältnismäßigkeitsgrundsatz (Erforderlichkeit)
5. Grundsatz der Transparenz der Datenverarbeitung

- genaue Regelungen hierzu im DSG NRW

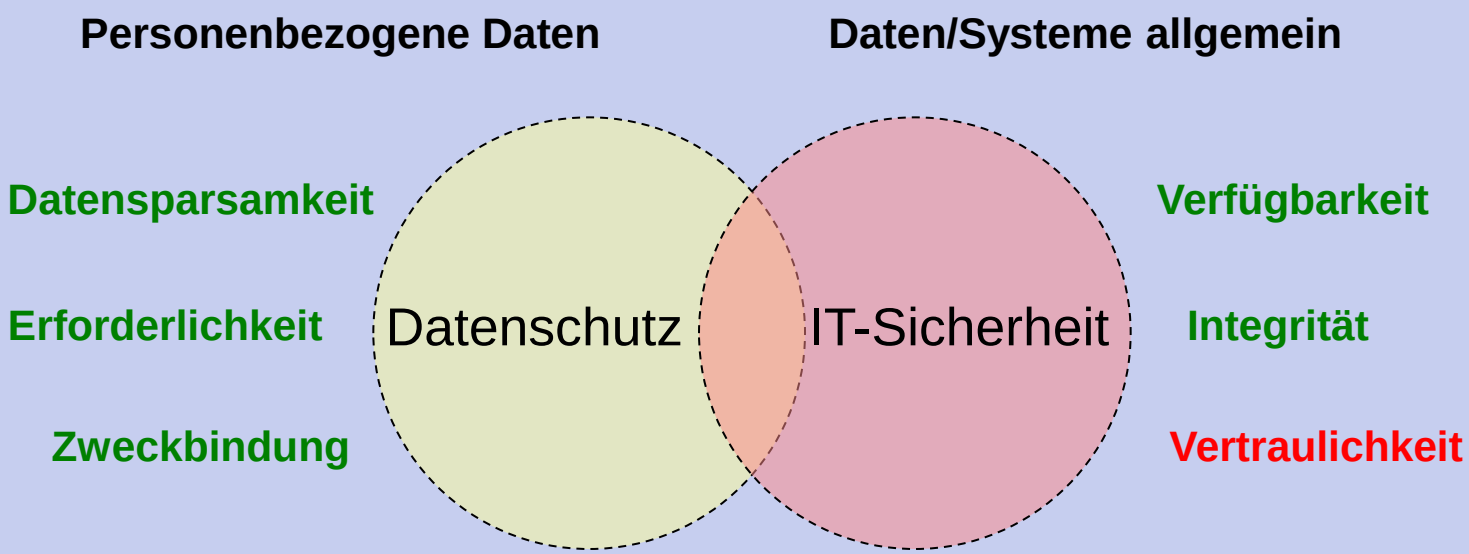
Vorabkontrolle und Verfahrensverzeichnis

- Überprüfung eines IT-Verfahrens, welche personenbezogene Daten verarbeitet werden, auf die Einhaltung der datenschutzrechtlichen Vorschriften
- Verfahrensverzeichnis ist Grundlage
  - Zweckbestimmung und Rechtsgrundlage der DV
  - Art der gespeicherten Daten
  - Kreis der Betroffenen
  - Herkunft und Empfänger personenbezogener Daten
  - Zugriffsberechtigte Personen
  - Techn. und organisatorische Maßnahmen
  - Löschfristen
  - Technik des Verfahrens

Sonderpunkte

- Datenverarbeitung im Auftrag
- Protokollierung zur Revisionssicherheit
- Auskunftsersuchen von Behörden und Dritten

Datenschutz und IT-Sicherheit



Sicherheitszwischenfälle (Auszug)

2008

- SPAM-Versand über einen Webserver der **Biologie**
- Webserver des **CeBiTec** über Sicherheitslücke gehackt
- Störung der Stromversorgung im **HRZ**

2009

- Wurm auf den Hallendisplays der **Verwaltung**
- Trojaner entwendet E-Mails und Zugangsdaten dem Notebook eines **CITEC**-Professors
- Rechner-Diebstähle in **Hörsälen**

Zwischenfälle und ihre „Meldung“

Artikel

SPIEGEL

PANNE DER UNI MAGDEBURG

Daten von 44.000 Studenten aus Versehen im Web

SPIEGEL ONLINE - 27.05.2008

Datenstriptease deluxe: Zehn Tage lang konnte sich jeder detailliert über Magdeburger Studenten und Absolventen informieren. Ein Mitarbeiter wollte an der Uni-Datenbank schrauben - und parkte die sensiblen Informationen auf einem ... mehr...

News (Schweiz/Security)

Donnerstag, 17. Juli 2008

Uni Basel Opfer einer Phishing-Attacke

Ohne gross nachzudenken haben Studenten ihre Zugangsdaten Preis gegeben, weil sie in einem E-Mail dazu aufgefordert wurden.

Studenten der Uni Basel sind, wie das eigene Universitätsrechenzentrum berichtet auf eine

SICHERHEIT / NEWS Weitere News

05.10.2009 PDF | E-Book | | RSS

Noch immer mehr als 5 Millionen Rechner infiziert

Conficker legt Universität lahm

Der Wurm Conficker ist noch immer aktiv und richtet Unheil an. Nun hat es die Universität Oxford Brookes erwischt - betroffen waren vor allem öffentlich zugängliche PCs.

Es ist ruhig geworden um den Wurm Conficker, der es Anfang des Jahres noch in die Schlagzeilen der internationalen Tagespresse geschafft hat. Eine Infektion an der Universität Oxford Brookes zeigt allerdings, dass die *Malware* noch immer quicklebendig ist. Die Vertreter der Universität sahen sich gezwungen, einen Großteil des Netzwerks lahm zu legen, um die Infektion zu bekämpfen.

02.10.2008 Drucken | Senden | Bookmark | Feedback | Merken

UNI GÖTTINGEN Schrift: - +

Datenpanne mit Namen von 26.000 Studenten

Hacker haben die Universität Göttingen auf ein peinliches Leck aufmerksam gemacht: Offenbar monatelang waren die Namen von 26.000 Studenten ungeschützt auf einem Server zugänglich - und hätten zu einem riesigen E-Mail-Verteiler werden können.

Durch eine Sicherheitslücke auf einem zentralen Server der Universität Göttingen waren bis zur Nacht von Mittwoch auf Donnerstag Daten von rund 26.000 Studenten öffentlich zugänglich. Offenbar blieb kein Göttinger Student von der Panne

Beispielhafte Gründe für Zwischenfälle

- Begrenzte **IT-Ressourcen** (Beschäftigte)
- **Teilzeit**-Administratoren mit hoher Fluktuation
- Mangelndes Sicherheits-Know How und -**Bewusstsein**
- Fehlende **Kenntnis** der Regelungen zur IT-Sicherheit
- Zeitintensiver **Eigenbetrieb** vieler Einzeldienste
  - E-Mail Server
  - Benutzerverwaltung
  - Backup Dienste
  - Web Server
  - …

IT-Sicherheitsleitlinie

- Die Verantwortung für die IT-Sicherheit jeder Fakultät oder Einrichtung liegt bei der jeweiligen **Leitung**.

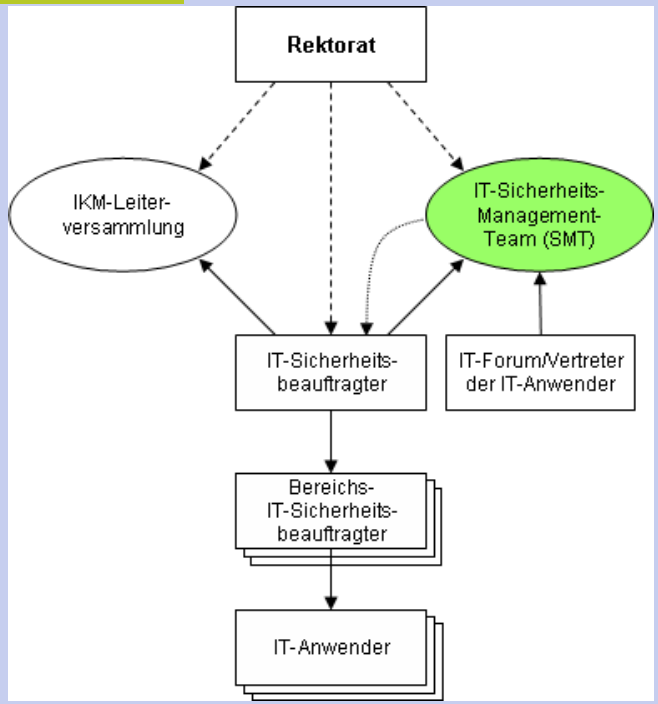
- IT-Sicherheitsprinzipien (Auszug)
  - IT-Systeme werden in einer **sicheren** Umgebung betrieben
  - Die **administrative** Arbeit auf IT-Systemen wird sicher und nachvollziehbar gestaltet
  - Informationen werden ihrer **Kritikalität** entsprechend angemessen sicher verarbeitet
  - IT-Systeme werden durch **kompetentes** Personal langfristig betreut

Bedrohung, Risiken und Maßnahmen

- Bedrohungen erkennen
  - Fehlerhaftes Verhalten, Malware, externe Angreifer, höhere Gewalt (Brand, Unwetter, Todesfall)
- Risiken einschätzen
  - Schutzbedarf: Wie **kritisch** sind Systeme & Informationen für mich?
  - ggf. **Risikoanalyse** durchführen: Risiken im Detail betrachten
- Maßnahmen ergreifen um Risiken zu reduzieren
  - Technische Maßnahmen: Virenschutz, Firewall, Verschlüsselung etc.
  - Organisatorische Maßnahmen: Einheitliche **Regelungen** und Prozesse etablieren, Sicherheitsbewusstsein bei den Beschäftigten aufbauen

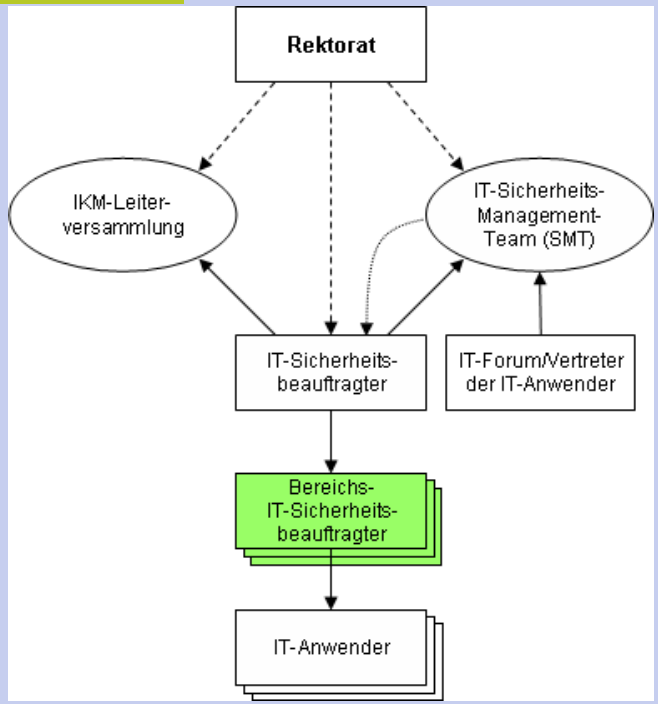
IT-Sicherheitsorganisation: SMT

- Setzt sich aus Vertretern einzelner **Bereiche** und Funktionen zusammen
- **Berät** den IT-Sicherheits-beauftragten
- Übt **steuernde** und kontrollierende Funktionen im IT-Sicherheitsprozess aus



IT-Sicherheitsorganisation: BITS

- Tragen Bereichs-**Verantwort-ung** im IT-Sicherheitsprozess
- Wirken bei **Umsetzung** von Konzepten & Maßnahmen mit
- Prüfen **Wirksamkeit** und Einhaltung der Maßnahmen
- Informieren über sicherheits-relevante **Vorkommnisse** und Schulungsbedarfe



Bisherige Schritte im IT-Sicherheitsprozess

- Verabschiedung **IT-Sicherheitsleitlinie** durch Rektorat
- Aufbau **IT-Sicherheitsorganisation**
  - IT-Sicherheitsbeauftragter
  - IT-Sicherheits-Management-Team (SMT)
  - Bereichs-IT-Sicherheitsbeauftragte (BITS)
- Erstellung **IT-Verfahrensübersicht** (welche Verfahren wo und durch wen verantwortlich betreut)
- **Schulungen** der Beschäftigten (Awareness)
- Erstellung von **IT-Sicherheitsrichtlinien** (Datacenter, VoIP, Firewalls etc.)

Weitere Schritte im IT-Sicherheitsprozess

- Erstellung verbindlicher **IT-Basisschutzregelungen**
- Festlegen von IT-Verantwortlichkeiten durch ein **Rollenmodell**
- Festlegung einheitlicher IT-Sicherheits-**Standards**
- Festlegung eines verbindliche Vorgehens zur **Dokumentation** von IT-Prozessen / IT-Verfahren und des dazugehörigen IT-Einsatzes
- Einführung von **Werkzeugen** für die Bewertung von IT-Verfahren (Schutzbedarf, Risikoanalyse)

Ziel: Durchgängiger IT-Sicherheitsprozess

1. Einheitliche **Verantwortlichkeiten** durch Rollenmodell
2. Einheitliche **IT-Basissicherheit** durch IT-Basisschutz
3. Einheitlicher **Dokumentationsprozess** der IT-Verfahren
4. Einheitlicher **Bewertungsmaßstab** durch Schutzbedarfs- und Risikoanalyse

Herzlichen Dank…

Haben Sie Fragen?