Datenschutz- und IT-Sicherheitsaudit

Eine Chance für das Gesundheitswesen

54. GMDS-Jahrestagung
Essen, 2009-09-09

Dr. Bernd Schütze

Agenda

1. Fragestellung
2. M&M
   a) Definition(en)
   b) Audit und BDSG
   c) Normen
3. Ergebnisse
   a) Vorteile
   b) Umsetzungen
4. Diskussion / Fazit

Fragestellung

- Daten – und insbesondere Gesundheitsdaten – sind auch für Unbefugte von Interesse
- Ohne Daten kann das “Geschäft” Gesundheitswesen nicht funktionieren
  - Behandlung
  - Nachweis der durchgeführten Behandlung
  - Abrechnung…

Wie kann die Sicherheit der Daten gewährleistet werden?

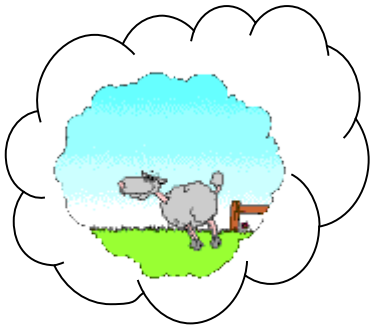
Definition(en)

- Daten sind Einzelangaben über Verhältnisse
- Personenbezogene Daten können einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)
- Erheben ist das Beschaffen von Daten
- Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten.
- Audit ist die Prüfung und Bewertung eines Konzepts sowie der technischen Einrichtungen durch unabhängige Gutachter

(Entsprechend BDSG)

Audit und BDSG

- 2001: Änderung BDSG, erstmals Datenschutzaudit ermöglicht, Konkretisierung sollte in eigenem Gesetz erfolgen
- Seitdem, nun ja…



Normen

- ISO/IEC 27001
  - Formulierung von Anforderungen und Zielsetzungen zur Informationssicherheit
  - Kosteneffizientes Management von Sicherheitsrisiken
  - Sicherstellung der Konformität mit Gesetzen und Regulatorien
  - Identifikation und Definition von bestehenden Informationssicherheits-Managementprozessen
  - Definition von Informationssicherheits-Managementtätigkeiten
  - Gebrauch durch interne und externen Auditoren zur Feststellung des Umsetzungsgrades von Richtlinien und Standards

(Internationale Norm seit 15. Oktober 2005)

Ausland?

- USA
  - verpflichtend durch Sarbanes-Oxley Act (SOX, 2002)
  - Health Insurance Portability and Accountability Act (HIPAA, 1996)
  - Audits entsprechend Vorgaben des American Institute of Certified Public Accountants (AICPA)
- Europa
  - Directive 95/46/EC (1995, Umsetzung bis 1998)
  - Deutschland = Datenschutzgesetze
- Österreich
  - Gesundheitstelematikverordnung (GTelV)

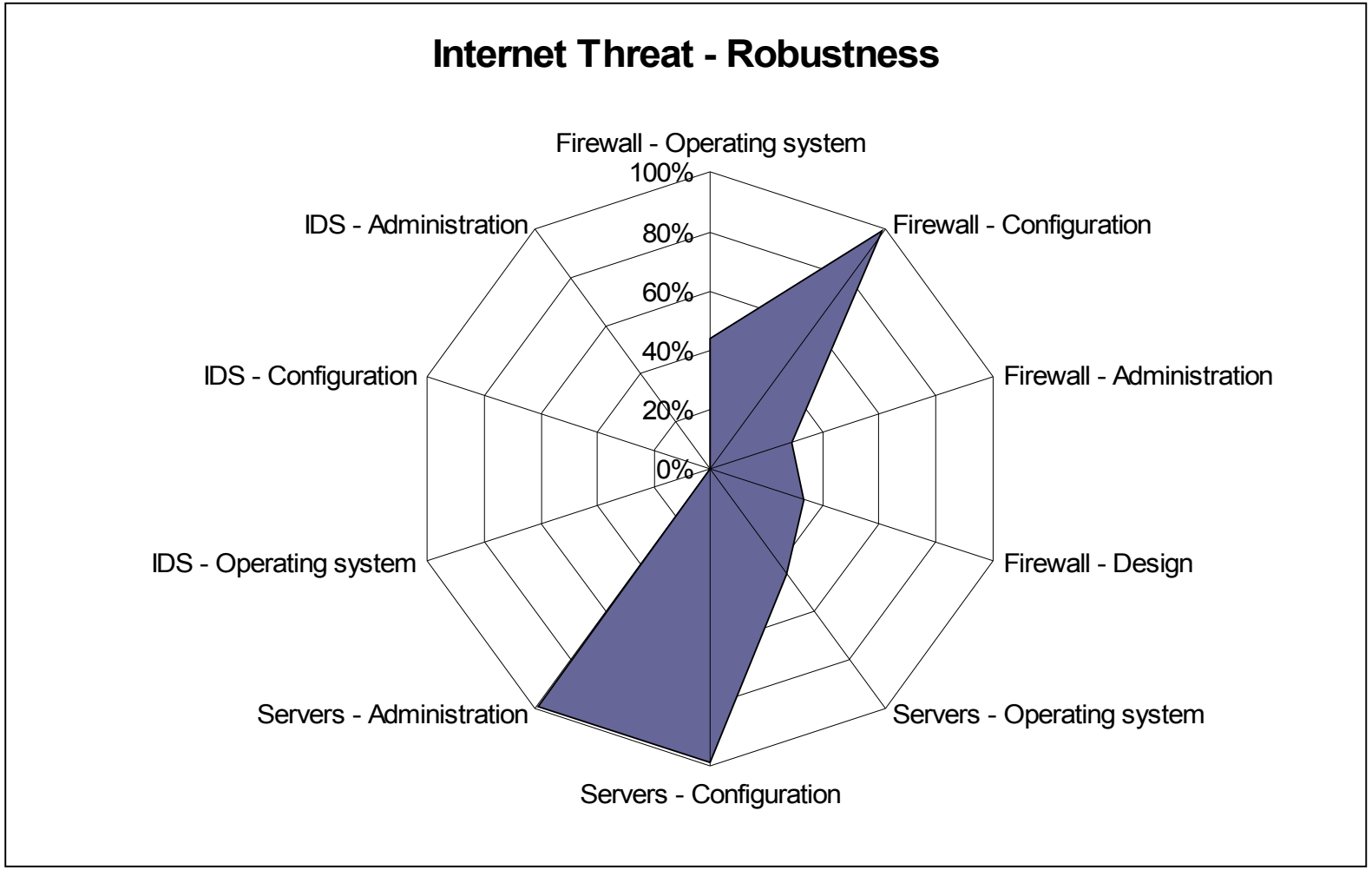
Procedere

- Organisation:
  - Policies
  - Prozesse
  - sonstige Dokumente (Inventare, Pläne, Konzepte etc.)
- Technik:
  - Physische Sicherheit
  - Netzwerksicherheit
  - Systemsicherheit
  - Applikationssicherheit

Wichtig: Untersuchungstiefe vor Beginn bestimmen

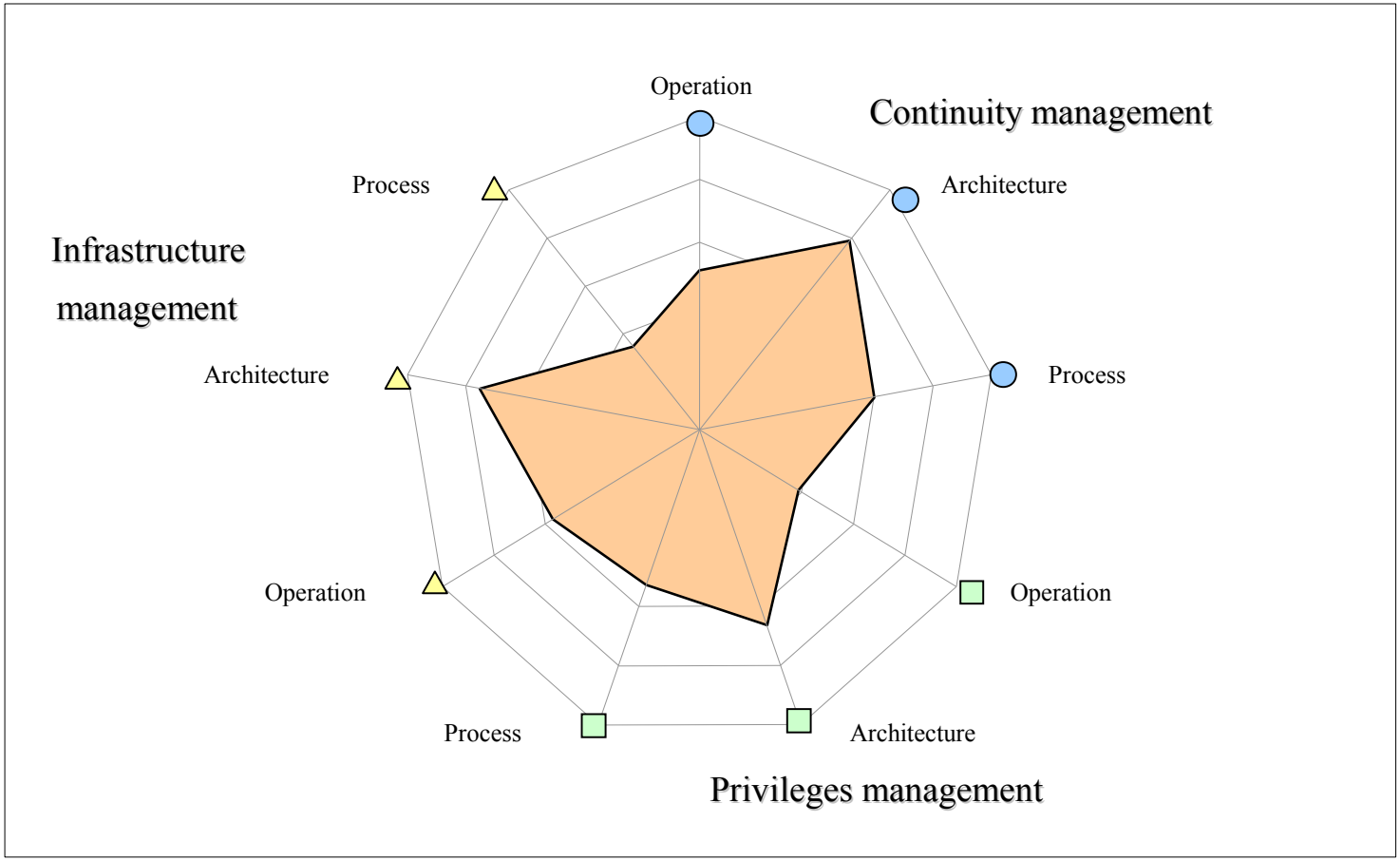
Beispiel Risikoanalyse

- Fragestellung
- Definition(en)
- Audit & BDSG
- Normen
- Vorteile
- Umsetzungen
- Diskussion



Beispiel Prozessanalyse

- Fragestellung
- Definition(en)
- Audit & BDSG
- Normen
- Vorteile
- Umsetzungen
- Diskussion



Vorteile

- Proaktives Vorgehen
- Entscheidungsgrundlage für Riskomanagement
  - Soll- und Ist-Zustand wird dargelegt
  - Geschäftsführung und IT-Abteilung definieren Sicherheitsniveaus für Daten
  - Kosteneffizientes Risikomanagement wird ermöglicht
  - To-Do-Liste mit Prioritätsniveau
  - (Don‘t-Do-Liste)
- Darstellung für Partner und Kunden
- Sicherheit für die eigenen Mitarbeiter
- Nachweis im Schadensfall

Umsetzungen

Abbildung in der Wirklichkeit:
Ist doch im Gesundheitswesen nicht nutzbar…

… wussten einige wohl nicht

Krankenhaus

- Städtisches Klinikum Braunschweig gGmbH (BSI)

Rechenzentren

- perdata
- FIDUCIA IT AG
- T-Systems

Pharmakologie

- Bayer Health Care

Versicherungen

- Gothaer Krankenversicherung AG

Informationssystem-Hersteller

- ?

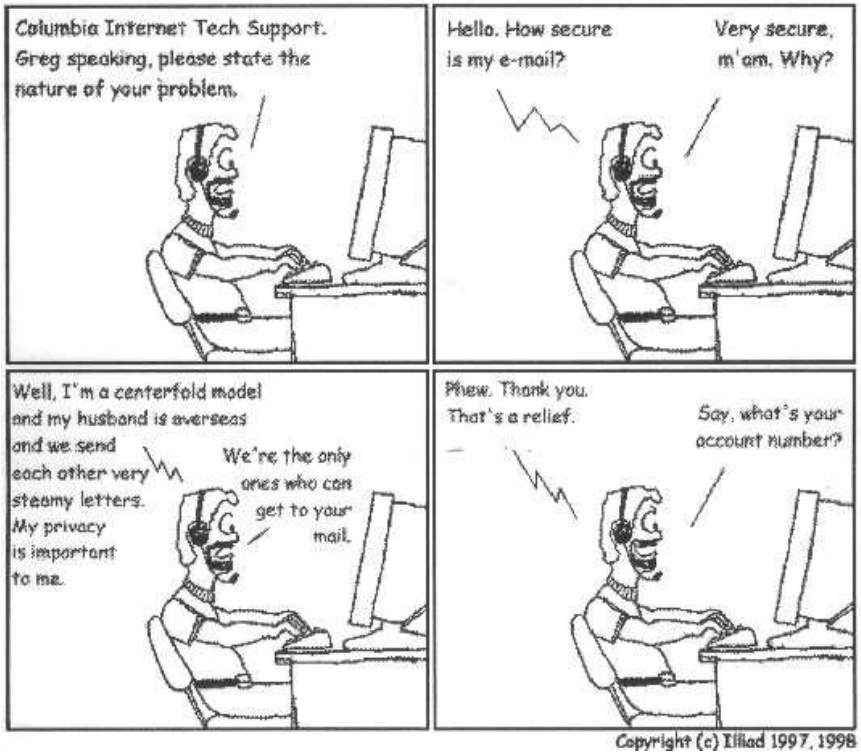
Fazit

- IT-Sicherheitsaudit
  - Datensicherheit optimiert
  - Gewährleistung für die anvertrauten Daten erhöht (Partner-, Kunden- und Mitarbeiterzufriedenheit ↑)
  - Vermeidung unerwünschter Werbung
- » Nachteil«: erhöhte Transparenz
  - Nicht alle wollen Transparenz

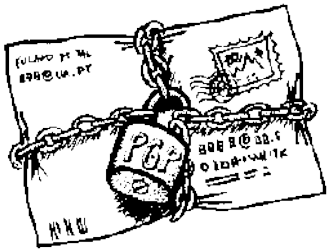
Fazit

Cave:

100%ige Sicherheit kann es nicht geben



Diskussion / Fragen ?



schuetze@medizin-informatik.org