Master-Thesis

Evaluation der Skalierbarkeit eines branchenspezifischen IT-Sicherheitsstandards durch ein IT-Grundschutzprofil am Beispiel des B3S "Medizinische Versorgung"

Fakultät für Ingenieurwissenschaften
B3S „Medizinische Versorgung“/IT-Grundschutz
Michael Sondermann
E-Mail: michael.sondermann@stud.hs-wismar.de
www.hs-wismar.de

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Agenda

- Einführung
  - Motivation / Historisches / Zielsetzung
- Grundlagen
- Rahmenbedingungen
- Mapping des B3S auf den IT-Grundschutz
- Technische Evaluation
- Fazit und Ausblick

Einführung

Motivation / Historisches / Zielsetzung

Die Vernetzung aller Systeme/IT-Systeme in allen Bereichen, bezeichnet mit „xxx 4.0“ und der daraus folgenden strukturierten Verknüpfung der anfallenden Daten:

- eröffnet **Möglichkeiten** und beinhaltetet **Entwicklungspotential**.
- Allerdings eröffnen sich durch die Vernetzung und den daraus folgenden **Barriere-Verlust** zwischen den Systemen **Risiken** die es zu beherrschen gilt.

Einführung

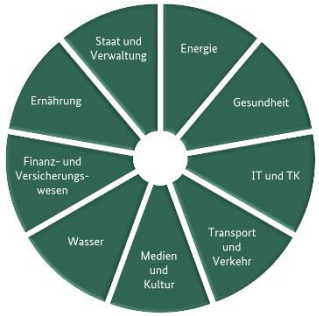
Motivation / Historisches / Zielsetzung

- Beruflicher Werdegang des Autors
  - 2002 – 2003 Systemadministrator Fachkrankenhaus (150 Betten)
  - 2003 – 2006 Bereichsleiter EDV, Fachkrankenhaus (150 Betten)
  - 2006 – 2016 Leiter-EDV, Akut-Krankenhaus der Schwerpunktversorgung (350 Betten)
  - 2016 – 2021 Leiter Informationstechnologie (CIO), Krankenhauskonzern (500 Betten + 110 in DL)
- Heute besteht eine fast vollständige Durchdringung aller Krankenhausprozesse mit Informationstechnologie.

=> **Der IT-Sicherheit kommt, für das funktionieren eines Krankenhauses, extrem hohe Bedeutung zu!**

Einführung

Motivation / Historisches / Zielsetzung



- 2015 - IT-Sicherheitsgesetz

  → Kritische Infrastrukturen (KRITIS) Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen…

- 2016 - BSI-KritisV

  → Bis 2019 ausschließlich Krankenhäuser mit min. 30.000 stationären Fällen pro Jahr. → Aufstellung eines B3S

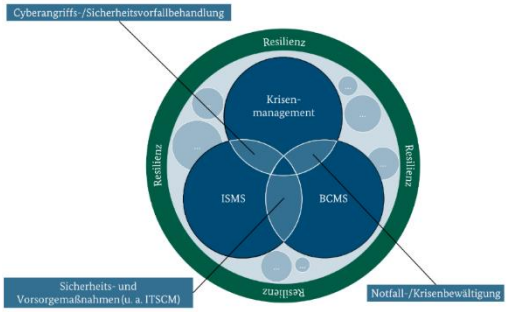
- 2020 - Änderung des Sozialgesetzbuch V durch das Patientendaten-Schutz-Gesetz

  → Verpflichtung **aller** Krankenhäuser zur Umsetzung eines dem Stand der Technik angemessenen IT-Sicherheitsstandards

- <u>Zielsetzung:</u>

Besteht für kleine bis mittelgroße Krankenhäuser die Möglichkeit die Anforderungen des B3S „Medizinische Versorgung“ unter Anwendung des IT-Grundschutzes umzusetzen?

Grundlagen



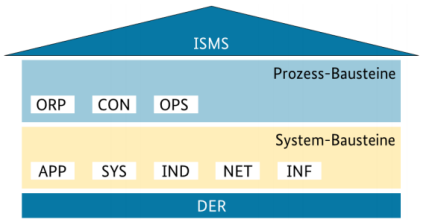
- Begrifflichkeiten und deren Abgrenzungen
  - **Sicherheitsmanagement**
    - Prozess der Planung, Konzeption, Umsetzung, kontinuierlichen Prüfung, …

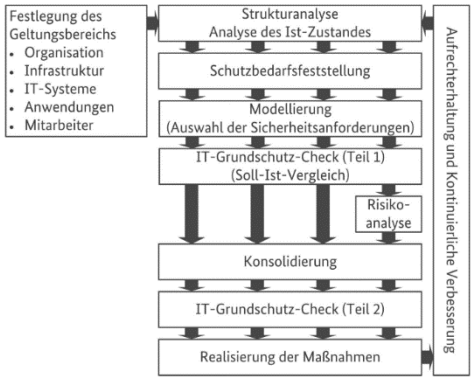
      → Gesamtunternehmen (Prozesse, Ressourcen, Organisation, Produkte und Dienstleistungen)
  - **Informationssicherheitsmanagement**
    - Einhaltung des Sicherheits-, Kontinuitäts- und Risikoniveaus von Informationen
  - **IT-Sicherheitsmanagement**
    - Prozess der Planung, Konzeption, Umsetzung, kontinuierlichen Prüfung, …

      → Informations- und Kommunikationstechnologie des Unternehmens
  - **Kontinuitätsmanagement (Business Continuity Management)**
    - Sicherstellen einer risikojustierte und jederzeit ausreichende Handlungsfähigkeit des Unternehmens
  - **Risikomanagement**
    - Erhebung, Analyse, Bewertung, Justierung, Behandlung, Überwachung… von Risiken

Grundlagen

- Informationssicherheit versus IT-Sicherheit
  - Schutz von Informationen (in Köpfen auf Papier, **in** IT-Anlagen) **versus** Schutz **von** eingesetzten Informationstechnischen Systemen
- B3S als „Stand der Technik“ im Sektor Gesundheit
- BSI-Standards, hier → 200-2 „IT-Grundschutz-Methodik“
  - Konkreter Aufbau eines ISMS nach IT-Grundschutz-Standard
  - Basis-, Kern- und Standardabsicherung
  - Risikobewertung bereits enthalten
- IT-Grundschutz-Kompendium
  - Prozess-Bausteine
  - System-Bausteine
- Vorgehensweise zur Umsetzung
  - nach Standardabsicherung





Rahmenbedingungen

- Auf Grundlage des B3S und IT-Grundschutz

  → Vorbetrachtung und Festlegung der Rahmenbedingungen zum Mapping zwischen Anforderungen des B3S und der Systematik nach IT-Grundschutz / BSI-Standard 200-2 “IT-Grundschutz-Methodik“

- Methodik zur Erstellung des B3S → gem. Orientierungshilfe – B3S

1. Informationssicherheitsmanagement nach ISO 27001 als Grundlage des B3S → ISO konform (B)+(S) ✓
2. Abgrenzung des Geltungsbereichs → *BSI Standard 200-2 „Festlegung des Geltungsbereichs“* ✓
3. Erhebung der Anforderungen an ein ISMS nach ISO 27001 und ISO 27799 → *ISO konform* ✓
4. Identifikation der relevanten gesetzlichen Anforderungen zu den kDL im B3S-Geltungsbereich ✓
5. Identifikation ggf. anwendbarer Sicherheitsstandards mit Bezug zur IT- und Informationssicherheit ✓
6. Klassifikation der erhobenen Anforderungen

   → Informationssicherheit (B3S) vs. konkrete Maßnahmen der IT-Sicherheit (Grundschutz) ✓
7. *Anpassung von Inhalt und Strukturierung B3S gemäß B3S-Orientierungshilfe* *(✓)*

Rahmenbedingungen

- Überprüfung der Anforderungen des B3S

  → speziell auf Umsetzbarkeit der IT-Sicherheit überprüft!

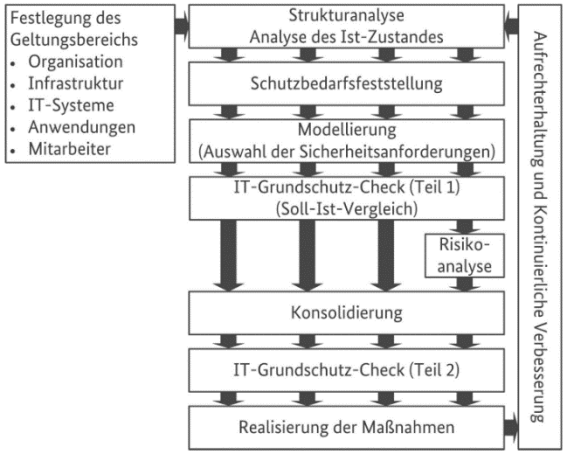
  - Der B3S „Medizinische Versorgung“ geht von fehlender Standardisierung im Krankenhaus aus

    → IT-Grundschutz ist „Stand der Technik“ für typische Geschäftsbereiche und Anwendungen

  - B3S „Medizinische Versorgung“ gem. § 8a (1) BSI-Gesetz durch das BSI anerkannt

    => Prüfgrundlage bei der Umsetzung in der Praxis

  - Empfohlene Schritte zur Umsetzung gem. B3S
    1. Kontext des ISMS definieren
    2. Managementstruktur für ISMS definieren
    3. Grundsätzliche Maßnahmen umsetzen
    4. Bestandsaufnahme, Risikoeinschätzung und Konzeption
    5. Umsetzung der Maßnahmen (von detailliertem Plan zur Risikobehandlung)
    6. Projektbegleitende Trainings, Ausbildung und Awareness
    7. Evaluierung der Effektivität des ISMS



Mapping des B3S auf den IT-Grundschutz

- Mapping der Anforderungen des B3S auf die Methodik des IT-Grundschutz

  → vor dem Hintergrund der Umsetzbarkeit der IT-Sicherheit

- *B3S* → *„was und ggf. womit ist zu schützen“*
- *IT-Grundschutz* → *„wie ist zu schützen“*

Anforderungen aus dem B3S

→ Mapping auf IT-Grundschutzbausteine

→ (B) Basis-Anforderung / (S) Standardanforderung / (H) Anforderung bei erhöhtem Schutzbedarf

→ Beurteilung des durchgeführten Mappings

Mapping des B3S auf den IT-Grundschutz

ANF-MN 97 Für Fernzugriffe MÜSSEN sichere Kommunikationsverbindungen verwendet werden und deren Anforderungen SOLLEN regelmäßig kontrolliert werden.

OPS.1.2.5.A8 Sichere Protokolle bei der Fernwartung (S)

- Nur als sicher eingestufte Kommunikationsprotokolle SOLLTEN eingesetzt werden. Dafür SOLLTEN sichere kryptografische Verfahren eingesetzt werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.
- Wird auf die Fernwartungszugänge von IT-Systemen im internen Netz über ein öffentliches Datennetz zugegriffen, SOLLTE ein abgesichertes Virtuelles Privates Netz (VPN) genutzt werden.

Die Anforderungen aus ANF-MN 97 des B3S lassen sich mit den ausgewählten Formulierungen aus den IT-Grundschutz-Baustein-Anforderungen gem. OPS.1.2.5.A8 abbilden. Anzumerken ist, dass eine Umsetzung gem. Grundschutz-Baustein in Kombination mit dem B3S erfolgt und somit das „SOLLTE“ durch ein „MUSS“ zu ersetzen ist.

Technische Evaluation

- Evaluation anhand der Infrastruktur eines Krankenhauses aus dem Verbund der Friesland Kliniken gGmbH

  → Standort der Schwerpunktversorgung mit 350 Betten

- Für ausgesuchte Teilbereiche Evaluation des Mappings, mit dem Schwerpunkt der Umsetzung von IT-Sicherheit gem. B3S

  → Phase der Modellierung (Auswahl der Sicherheitsanforderungen)

Kernprozesse im Geltungsbereich des B3S Vorbereitung/Aufnahme

- Diagnostik
- Therapie
- Unterbringung und Pflege
- Entlassung

Technische Unterstützungsprozesse

- Informationstechnik (IT)
- Kommunikationstechnik (KT)
- Medizintechnik (MT)
- Versorgungstechnik (VT)

Kritische branchenspezifische Anwendungssysteme
→ „Zielobjekte“

- Krankenhausinformationssystem (KIS)
- Laborinformationssystem (LIS)
- Radiologieinformationssystem (RIS)
- Picture Archive an Communication System (PACS)
- …

Technische Evaluation

Zielobjekte Informationstechnik

Zielobjekt des Unterstützungsprozesses	IT-Grundschutz-Bausteingruppen
Arbeitsplatzsysteme (z.B. PC-Arbeitsplätze, Befund-Arbeitsplätze, Notebooks, Tablets, Smartphones) über den Lebenszyklus	SYS.2 Desktop-Systeme SYS.3 Mobile Devices SYS.4 Sonstige Systeme
Serversysteme (Anwendungen, Datenbanken, Basisdienste, z. B. Verzeichnisdienste, DNS, DHCP)	APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 ACTIVE DIRECTORY APP.2.3 OpenLDAP APP.3.2 Webserver APP.3.3 Fileserver APP.3.4 Samba APP.3.6 DNS-Server APP.4.6 SAP-ERP-Systeme APP.4.2 Relationale Datenbanken APP.5.2 Microsoft Exchange und Outlook APP.5.3 Allgemeiner E-Mail Client und Server SYS.1.1 Allgemeine Server SYS.1.3 Sever unter Linux und Unix NET.4.3 Faxgeräte und Faxserver

Zielobjekt des Unterstützungsprozesses	Technische Ausprägung
Arbeitsplatzsysteme (z.B. PC-Arbeitsplätze, Befund-Arbeitsplätze, Notebooks, Tablets, Smartphones) über den Lebenszyklus	Es kommen in der Fläche Windows-basierte FAT-Clients zum Einsatz. Vereinzelte THIN-Clients sind in Betrieb und der Einsatz von THIN-Clients soll ausgebaut werden. Notebooks sind teilweise im Bereich der mobilen Visite, für Homeoffice Arbeitsplätze und Mitarbeiter*innen mit häufig wechselnden Arbeitsorten innerhalb des Krankenhausstandortes im Einsatz.
Serversysteme (Anwendungen, Datenbanken, Basisdienste, z. B. Verzeichnisdienste, DNS, DHCP)	Es wird ein zentrales ACTIVE DIRECTORY System der Firma Mircosoft incl. DNS, WINS und DHCP betrieben. Ein ERP-System der Firma data net solutions GmbH kommt ebenso zum Einsatz wie diverse Relationale Datenbanken, Webserver und ein Mircosoft Exchange System.

Zielobjekt Anwendungssystem

Betroffenes Anwendungssystem	IT-Grundschutz-Bausteingruppen
Krankenhausinformationssytem (KIS)	APP.3 Netzwerkbasierte Dienste APP.4.3 Relationale Datenbaken APP.6 Allgemeine Software SYS.1 Server

Komponenten des Zielobjektes Krankenhausinformationssytem (KIS)	Technische Ausprägung und anzuwendende IT-Grundschutz-Bausteingruppen
Datenbankserver	Das den Betrachtungen zugrundeliegende Krankenhaus setzt das KIS medico der Firma CGM ein. medico wird im Kern mit den vier hier dargestellten Serversystemen betrieben. Der Datenbankserver wird, wie alle nachfolgenden Server des KIS virtualisiert betrieben. Grundlage ist ein Linux- basiertes System mit einer relationalen Ingres Datenbank. Auf der beschriebenen Grundlage müssen für den Server folgende Bausteine bzw. Bausteingruppen erfüllt werden: APP.4.3 Relationale Datenbanken SYS.1.1 Allgemeine Server SYS.1.3 Server unter Linux und Unix

Fazit und Ausblick

- Die Vorgehensweise zur Umsetzung gem. B3S ist mit der Sicherheitskonzeption nach Standardabsicherung der IT-Grundschutz-Methodik weitgehend kompatibel. Vorteil ist die in der IT-Grundschutz-Methodik bereits enthaltene Risikobewertung.

- Die Anforderungen des B3S weisen eine methodisch etwas andere Strukturierung auf. Allerdings lassen sich, im Rahmen einer engeren Auslegung, die **Anforderungen des B3S durch die IT-Grundschutz-Systematik erfüllen**!

- Die Vorannahme, dass für den Bereich der eingesetzten Medizingeräte eine gesonderte Risikoanalyse erfolgen muss, hat sich nicht bestätigt. Die Geräte lassen sich voll umfänglich mit der Methodik des IT-Grundschutzes abbilden.

- Die Erkenntnisse der Arbeit könnten in einem nun anschließenden Schritt, die Grundlage zur Erstellung eines IT-Grundschutz-Profils für Krankenhäuser bilden.

Vielen Dank für Ihre Aufmerksamkeit