HEALTHCARE SECURITY

IT-Sicherheitsgesetz für KRITIS: Gesundheit und Transport

Projektverlauf

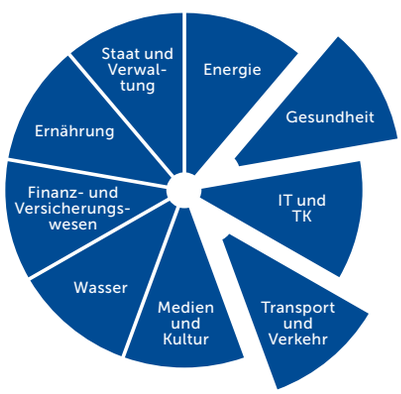
- Ganzheitliche Modellierung
- Security Audit
- Richtlinien
- Risikoanalyse
- Maßnahmen-katalog
- ISMS Implementierung
- Trainings
- ISMS Kontrolle

UP KRITIS – Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen

Bund und Länder unterscheiden neun Sektoren Kritischer Infrastrukturen. Zwei Sektoren sind vom ITSiG und der KRITIS-Verordnung betroffen.

› Gemäß **§8a** sind „**Betreiber Kritischer Infrastrukturen** verpflichtet [...] angemessene **organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen [...]".

› Dabei ist gemäß **§8a** der **„Stand der Technik"** einzuhalten, der branchenspezifisch definiert wird: **Branchenspezifischer Sicherheitsstand, B3S**



IT-Sicherheit nach B3S & ISO 2700x

B3S

DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG

Der Standard B3S definiert

› **168 Anforderungen** an Geschäftsführung und Verantwortliche

› **37 Anforderungen** für den Betrieb eines Informationssicherheits-Risikomanagements

› **50 Anforderungen** an Gefährdungsanalyse, unterteilt in allgemeine und IT-spezifische Bedrohungen

erfüllbar durch

ISO 27001/2/5 & ISO 27799

International etablierte Normen für Information Security Management Systeme (ISMS) und Risikomanagement

› **ISO 27001/2** beschreiben die Anforderungen an die Einführung, Implementierung, Wartung und kontinuierliche Verbesserung des **ISMS**

› **ISO 27005** definiert die Anforderungen an die **Identifikation, Bewertung** und **Behandlung** von **Risiken** bezüglich der Informationssicherheit

› **ISO 2799** ist eine **Erweiterung** der ISO 2700x um **krankenhaus-spezifische Anforderungen**

Projektverlauf „ICS Healthcare Security"

1 BESTANDSAUFNAHME

Security Audit
Abgleich mit gängigen Normen

› Managementstruktur ISMS: Verantwortlichkeiten, Lieferanten und Partner, Dokumentation und Datenschutz

› ISMS Kontext Erfassung: Leitlinie Informationssicherheit, Compliance-Anforderungen mit Stakeholder-Analyse

Ganzheitliche Modellierung
Modellierung aller Security-relevanter Bestandteile und eigens entwickelte Software, speziell zugeschnitten auf IT-Sicherheit

› Infrastruktur

› Technik

› Organisation

Statusbericht & Leitlinie Informationssicherheit

Ganzheitliches Modell

2 RICHTLINIEN

Managementstruktur ISMS
Entwicklung und Inkraftsetzung von Richtlinien

› Entwicklung

› Inkraftsetzung der ISMS Managementstruktur

Verfahren und Prozesse
Implementierung der Sicherheitsorganisation

› Entwicklung

› Inkraftsetzung der Verfahren und Prozesse

IT-Sicherheits-richtlinien

Verfahrens-anweisungen

Projektverlauf „ICS Healthcare Security"

3 RISIKOANALYSE

Bedrohungen und Schwachstellen
Top-Down Risikoanalyse für Gebäude, Systeme und Prozesse
› Identifikation von Bedrohungen und Sicherheitslücken
› Systematische Top-Down Analyse
› Berücksichtigung möglicher Sicherheitslücken für Krankenhaus-Bereiche, Personal und Patienten, medizinische Systeme

Risikobewertung
Analysen von Sicherheitslücken und Bedrohungen mit Risikobewertung
› Für alle Bedrohungen und Sicherheitslücken erfolgt eine detaillierte Risikobewertung
› Risikomatrix
› zusätzliche Schutzmaßnahmen

Angriffsbaum

Risikomatrix & Liste der Restrisiken

4 MASSNAHMENKATALOG

Maßnahmendefinition
Priorisierter Katalog für bauliche, technische und organisatorische Maßnahmen
› Reduktion von Risiken
› Verbesserung des ISMS

Gesamtkonzept
Sicht auf interne und externe Risiken führt zu vollständiger Absicherung
› Priorisierung und Umsetzungsplanung
› Begleitung des Unternehmens bei der Umsetzung
› Aufbau des ISMS

Maßnahmenkatalog & Abschlussbericht

Umsetzungsplan, Umsetzungsnachweise

5 AWARENESS

Trainings
Geschulte Mitarbeiter als wichtige Ressource zur Aufrechterhaltung der Sicherheit
› Schulungsbedarf ermitteln
› Mitarbeiterschulungen

ISMS Kontrolle
Begleitung bis zur Überprüfung der korrekten Umsetzung eines umfänglichen Sicherheitssystems
› Überprüfung und Weiterentwicklung
› Interne Audits

Schulungsunterlagen, Teilnahmeprotokolle

Aktualisierte ISMS Dokumente, interne Auditberichte

Referenzen

› DB, Projekt DiB:
Netzwerkkonzept: Modellierung Gebäude und Vernetzung
Spezifikationen: Security Anforderungen an sicherheitsrelevante Systeme und Prozesse
Betriebsführungskonzept: Beschreibung der Prozesse für sichere Betriebsführung, Gebäude- und IT-Management
› Deutsche Bahn:
Projekt DiB: TÜV-zertifizierte IT-Sicherheitsanalyse für das iLBS
Aktuell: Ausweitung der Analyse bis inkl. Stuttgart 21
› Schweizer Bundesbahnen, Projekt „SecRA eSTW": Bundesweite Risikoanalyse für die elektronischen Stellwerke (eSTW) inkl. ISMS Audit der SBB Organisation

› Unser ganzheitlicher Maßnahmenkatalog im Projekt DiB befindet sich bereits im Einsatz und ist TÜV-zertifiziert
› Mitarbeit an den Betriebsführungsvorgaben z.B. bei Patch- und Schwachstellen-Management oder Datenträgerprüfung
› Mehrere Projekte mit ISMS-Beratung und Zertifizierungsbegleitung
› Begleitet wurden bisher mehrere ISMS-Projekte von der Einführung bis zur Zertifizierungsbegleitung
› Die ICS bildet die verantwortlichen Fachkräfte aus und ist exklusiver Partner der DEKRA im Bereich Informationssicherheit

PATRIC BIRR
M. Sc., CISSP
Head of Business Center Security
Mobile: +49 172 728 05 80
E-Mail: Patric.Birr@ics-gmbh.de