1. Magdeburger Sicherheitsforum

Eine DIN-Norm für IT-Sicherheit

- Gesetze und Normen für Cybersecurity -

Dr. Hubert Feyrer <hubert.feyrer@autovision-gmbh.com>

MIS

AUTOVISION

Kurzvorstellung

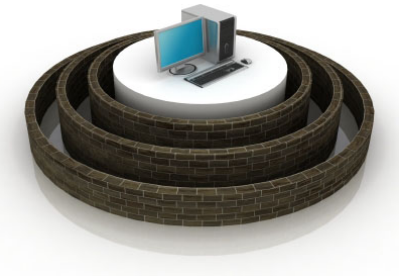
- Dr. Hubert Feyrer
- AutoVision GmbH

AUTOVISION

Über Informationen

Geschäftsprozesse

Anwendungen



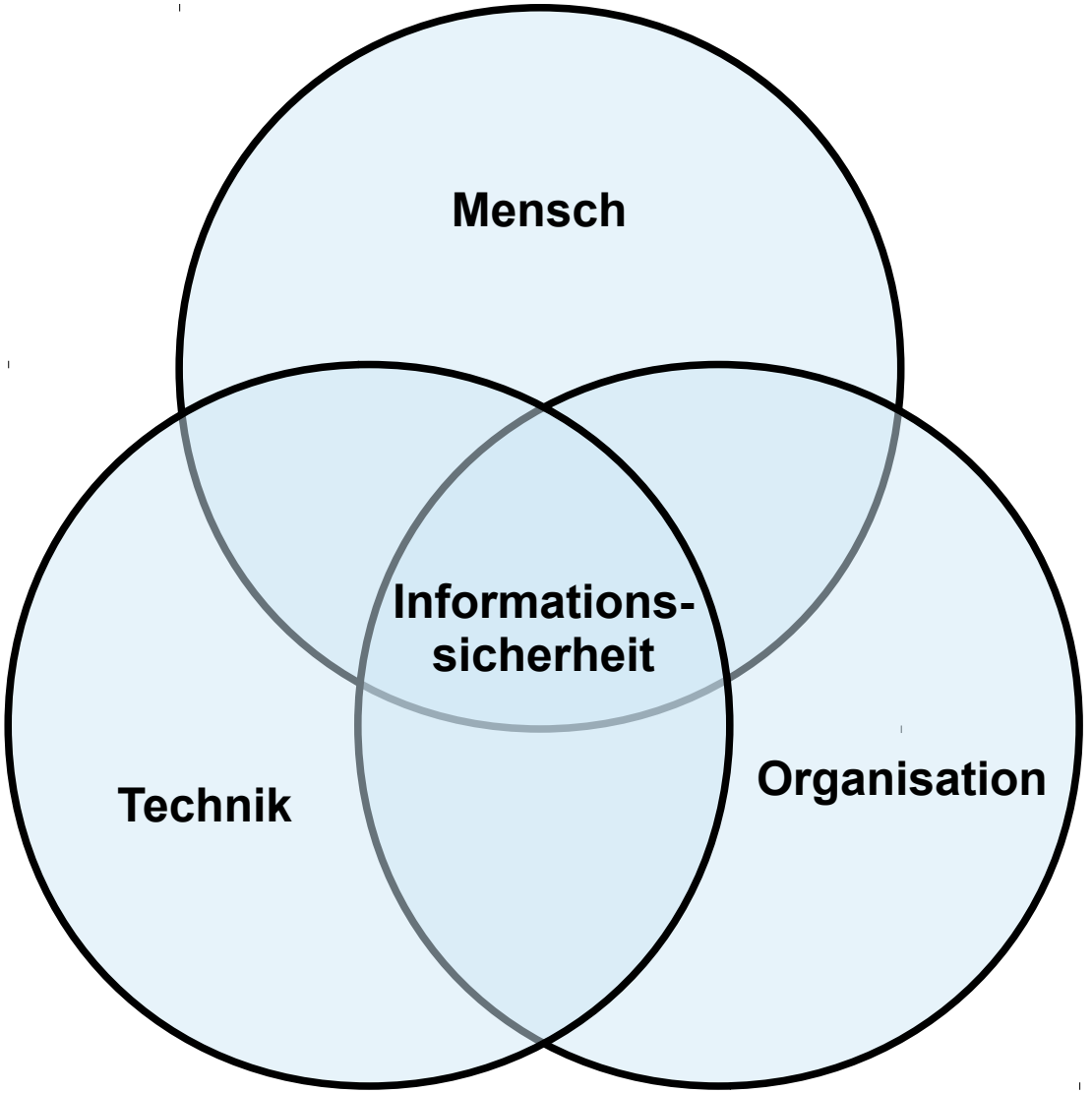
Informationen

Rechner

Infrastruktur – Speichersysteme, Netzwerk

MIS

AUTOVISION


Mensch
Informations-
sicherheit
Technik
Organisation

MIS

AUTOVISION

MIS

AUTOVISION

MIS

AUTOVISION

Ordnung

ist das halbe Leben...

...ich lebe in der anderen Hälfte!

MIS

AUTOVISION

MIS

AUTOVISION

Risikomanagement

Risiken:
Eintrittswahrscheinlichkeit
Folgen bei Eintritt

Sicherheit:
Geld
Zeit
Nerven

Wo anfangen?

Wo ist die DIN für IT-Sicherheit?

Naheliegende Optionen

Studium Jura!

- Bundesdatenschutzgesetz (BDSG)
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- Sarbanes Oxley Act (SOX), Basel II, Basel III
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Bilanzrechtsmodernisierungsgesetz (BilMoG)
- Mindestanforderungen an das Risikomanagement (MaRisk)
- Mindestanforderungen an Compliance und die weiteren Verhaltens-, Organisations- und Transparenzpflichten (MaComp)

Naheliegende Optionen

Studium Jura, Fortsetzung:

- Management-Haftung - AktG, GmbhG
- Sicherheitsüberprüfungsgesetz (SüG)
- Telekommunikationsgesetz (TKG), Teledienstgesetz (TDG), Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen (Vorrats-DS!)
- Handelsgesetzbuch (HGB), Buergerliches Gesetzbuch (BGB), Strafgesetzbuch (StGB)
- etc. etc. etc.

MIS

AUTOVISION

Naheliegende Optionen

Studium Informatik!

- IT Infrastructure Library (ITIL) – Best practices
- SPICE, CMMI, Common Criteria – SW-Entwicklung
- US National Institute of Standards and Technology (NIST) – Viele Standards um Sicherheit und Safety
- Payment Card Industry Standards (PCI)
- BSI IT-Grundschutz & Grundschutzkataloge
- ISO/DIN 27001 – ISMS (Informationssicherheitsmanagementsystem)
- CoBIT – Umfasst ISMS, ITIL, PMBOK, etc.

ISO/DIN 27001

- Festlegbarer Geltungsbereich (Scope)
- Festlegbarer Umfang (max. 133 Controls)
- Risikoanlyse
- Technische & Organisatorische Massnahmen, inkl. rechtlicher Auflagen und Sensibilisierung aller Mitarbeiter
- Management-System (vgl. ISO 9001)
- International anerkannte Norm
- International zertifizierbar

MIS

AUTOVISION

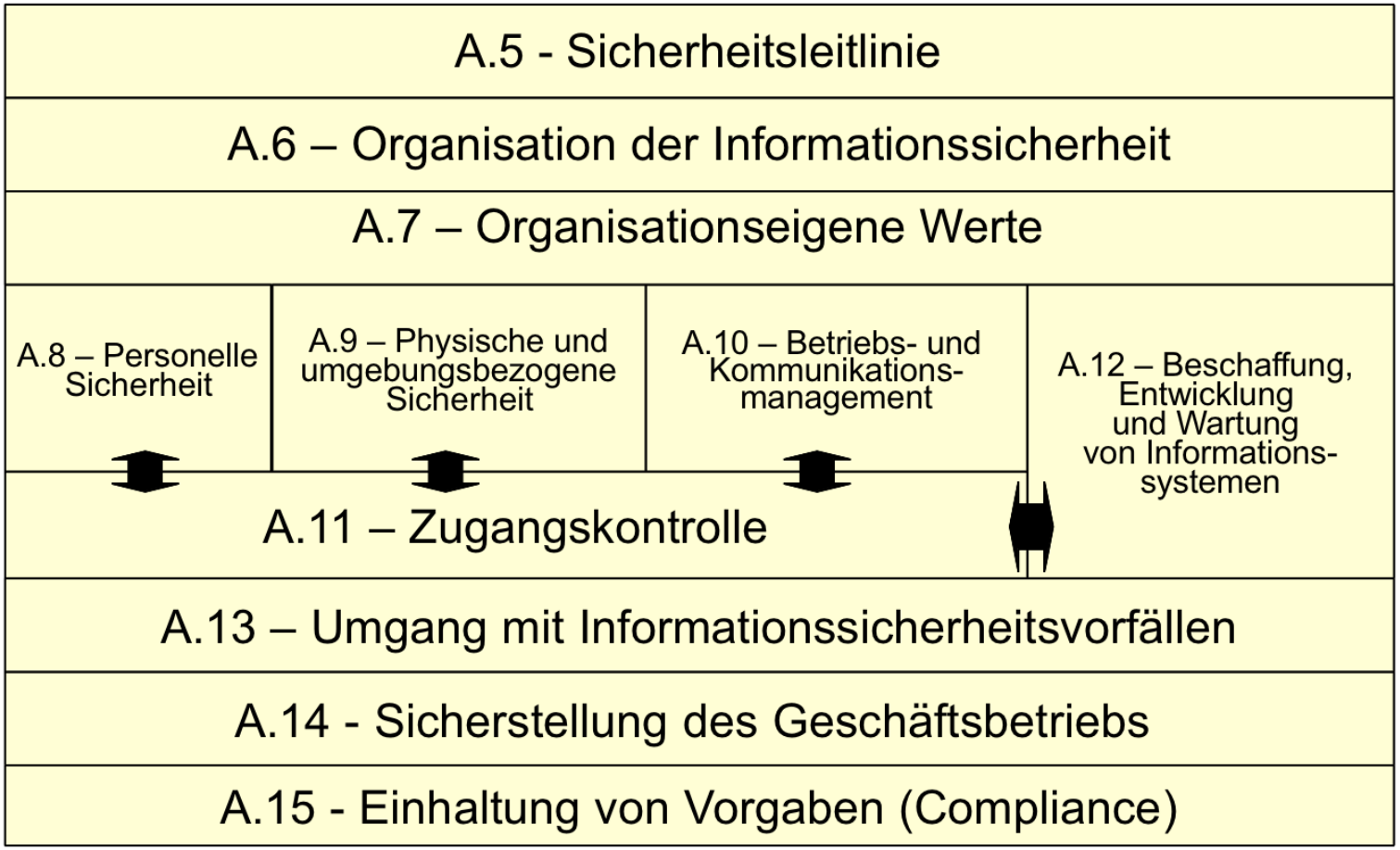
ISO 27032: Cybersecurity

ISO/IEC 27032 addresses “Cybersecurity” or “Cyberspace security”, defined as the **“preservation of confidentiality, integrity and availability of information in the Cyberspace”**. In turn “the Cyberspace” is defined as **“the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it**, which does not exist in any physical form”.

MIS

AUTOVISION

ISO 27001 Controls



MIS

AUTOVISION

Was davon MUSS ich umsetzen?

Nichts – aber es schläft sich besser!

MIS

AUTOVISION

Eine DIN-Norm für IT-Sicherheit

- Gesetze und Normen für Cybersecurity -

Fragen?

Kontakt: Dr. Hubert Feyrer
hubert.feyrer@autovision-gmbh.com
www.autovision-gmbh.com & www.feyrer.de

MIS

AUTOVISION