Informationssicherheit, Datenschutz, Urheberrecht

ISDS

Themenübersicht

01
Einführung EU-DSGVO

Datenschutz

erste Schritte EU-DSGVO

Artikel 4

02
Vertiefung EU-DSGVO

Kapitel 1
Art. 1 - 3

Kapitel 2
Art. 5 – 7, 9

Kapitel 3
Art. 12 - 23

Kapitel 4
Art. 25 - 32

03
Grundlagen Sicherheit

Schutzziele

BSI

Grundschutz

Standards

ISMS

ISO 27x

ISIS 12 für KMU

04
Angriff Abwehr

Layer 8 Problem

Angriffsvorbereitung

Schadsoftware

Sicherheitssoftware

05
Angriff Abwehr

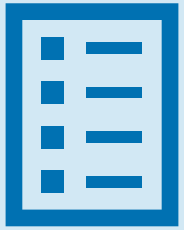
Angriffe auf Serverdienste

Brute Force

DoS & DDoS

Flooding

Tools



Agenda

- 01 Bedeutung von Sicherheit
- 02 Grundlegende Schutzziele und Maßnahmen
- 03 BSI
  - Einstieg
  - Standards
  - Grundschutz-Kompendium
- 04 Bedrohungen
- 05 Risiken
- 06 ISMS
- 07 ISO 27x

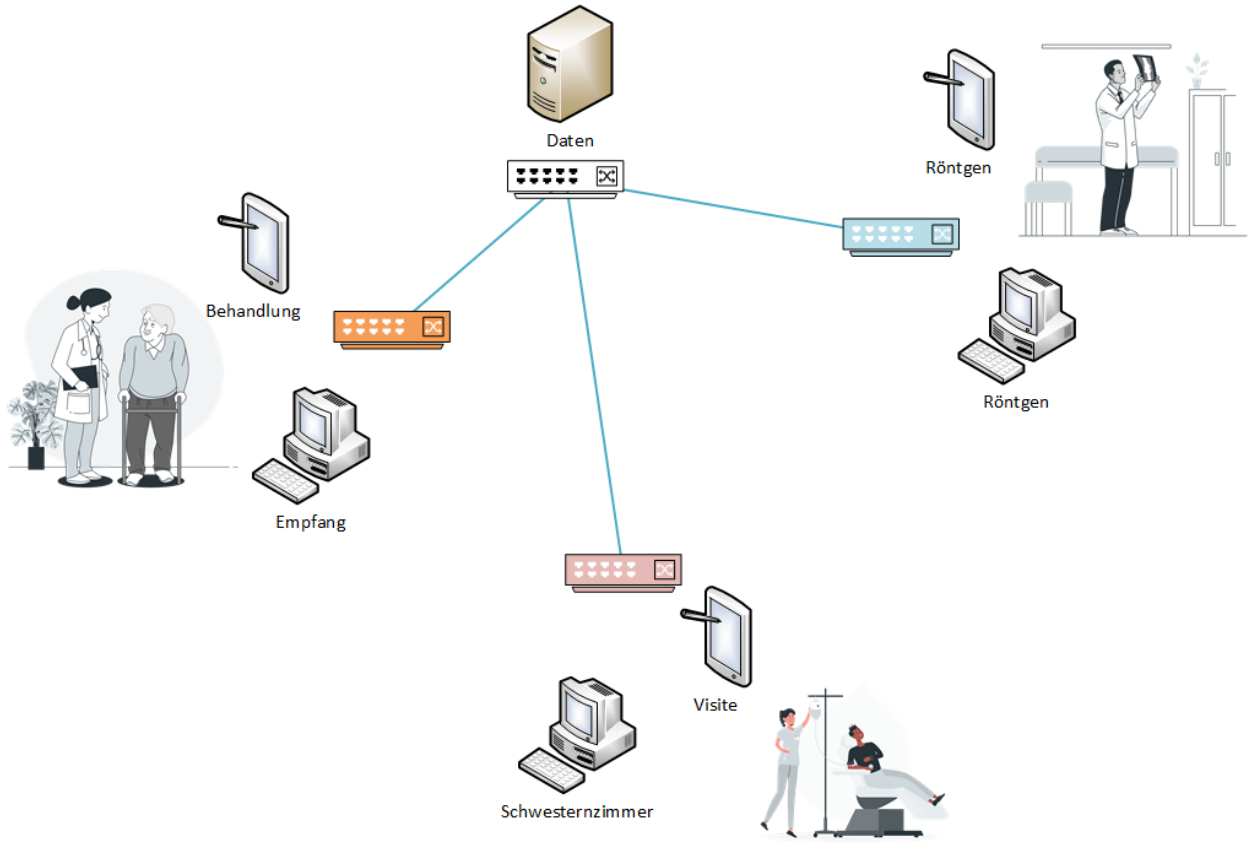
01 Bedeutung von Sicherheit

- *X*

01 Bedeutung von Sicherheit

- IT-Sicherheit
- Computersicherheit
- Datensicherheit
- Datensicherung

- So schnell wie sich die Technik entwickelt, verändern sich auch Sicherheitskonzepte



IT Infrastruktur in einem Krankenhaus (vereinfacht)

02 Grundlegende Schutzziele u. Maßnahmen

- *Ziele*
- *Maßnahmen*

02 Grundlegende Schutzziele und Maßnahmen

• Vertraulichkeit	Confidentiality
• Integrität	Integrity
• Verfügbarkeit	Availability
• Belastbarkeit (Resilienz) als Ergänzung	

02 Grundlegende Schutzziele und Maßnahmen

- Vertraulichkeit — Confidentiality

  Ein System gewährleistet Vertraulichkeit, sofern niemand unautorisiert Informationen gewinnen kann.

- Integrität — Integrity
- Verfügbarkeit — Availability
- Belastbarkeit (Resilienz) als Ergänzung

02 Grundlegende Schutzziele und Maßnahmen

- Vertraulichkeit — Confidentiality
- Integrität — Integrity

  Ein System gewährleistet die Integrität, sofern es nicht möglich ist, Daten unautorisiert und unbemerkt zu verändern. Gewährleistung der Ursprünglichkeit, Unverfälschtheit, Authentizität, Verbindlichkeit .

- Verfügbarkeit — Availability
- Belastbarkeit (Resilienz) als Ergänzung

02 Grundlegende Schutzziele und Maßnahmen

- Vertraulichkeit — Confidentiality
- Integrität — Integrity
- Verfügbarkeit — Availability

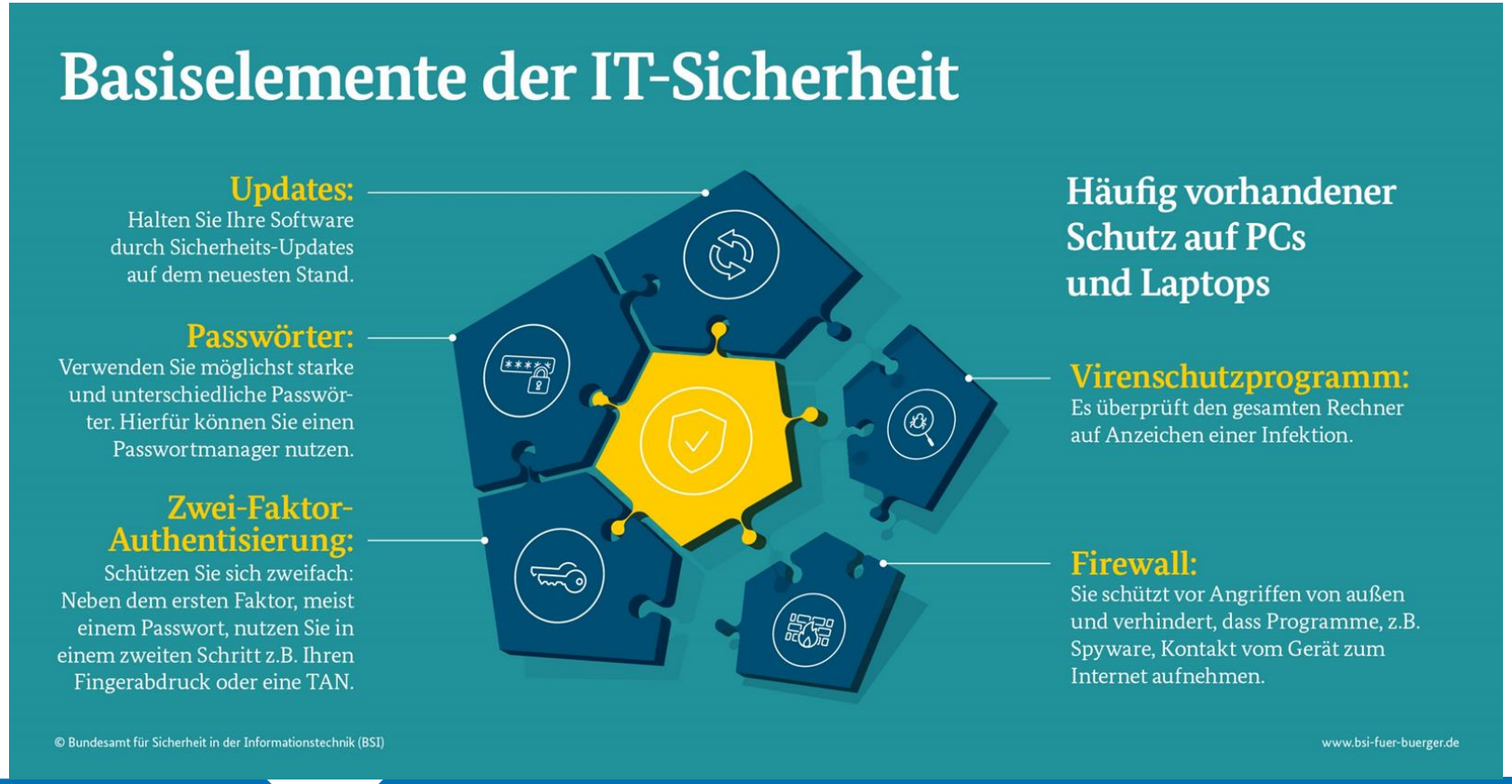
  Ein System gewährleistet die Verfügbarkeit, wenn Systeme redundant, ausfallsicher und wiederherstellbar abgesichert sind und über einen entsprechenden Schutz verfügen. Beispiele:
  - USV
  - Backup
  - Notfallplan
  - Krisenmanagement
- Belastbarkeit (Resilienz) als Ergänzung

03 BSI

- *Einstieg*
- *Standards*
- *Grundschutz-Kompendium*

03 BSI Bundesamt für Sicherheit in der Informationstechnik

Einstieg



03 BSI Bundesamt für Sicherheit in der Informationstechnik

Einstieg

Quelle: bsi.bund.de
(Bundesamt für Sicherheit in der Informationstechnik)

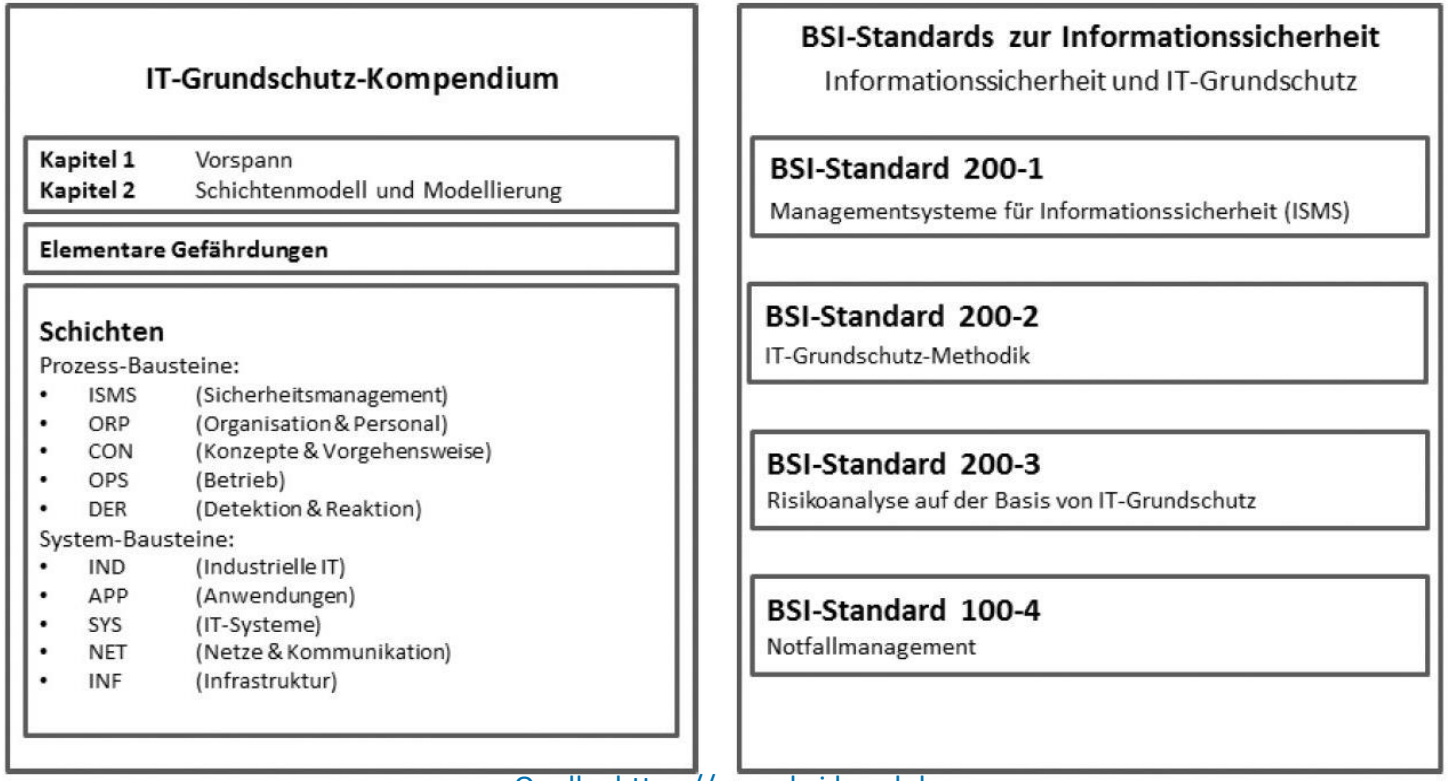
03 BSI Bundesamt für Sicherheit in der Informationstechnik

Einstieg

Quelle: bsi.bund.de
(Bundesamt für Sicherheit in der Informationstechnik)

03 BSI Bundesamt für Sicherheit in der Informationstechnik

Standards



Quelle: https://www.bsi.bund.de

03 BSI Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Kompendium

- Ziel, Idee, Konzeption
  - Schwachstellen
  - Bedrohungen
  - Gefährdungen

Trifft eine Bedrohung auf eine Schwachstelle, dann entsteht eine Gefährdung

03 BSI Bundesamt für Sicherheit in der Informationstechnik

Schwachstellen

- Physische Schwachstellen
- Natürliche Schwachstellen

- Schwachstellen von bzw. durch Hard- Software
- Schwachstellen von Medien
- Schwachstellen von Kommunikationsleitungen
- Schwachstellen durch Emissionen
- Schwachstellen durch Menschen

04 Bedrohungen

04 BSI Bundesamt für Sicherheit in der Informationstechnik

Bedrohungen

- USER
- Infrastrukturen
- Veraltete Technik
- Fehlendes Wissen
- Schadsoftware

04 BSI Bundesamt für Sicherheit in der Informationstechnik

Der User: Etwa 85 % aller erfolgreichen Angriffe auf IT-Systeme sind nur erfolgreich durch die bewusste oder unbewusste Mithilfe von Usern.

- Routine / Gewohnheiten
- Unbekümmertheit
- Manipulation
- sozial engineering
- Phishing
- Spam

05 Risiken

- *Risikomanagement*

05 Grundlagen Risikomanagement

- Ein Risiko kann als die Beschreibung eines Ereignisses mit der Möglichkeit negativer Auswirkungen definiert werden. Unbekümmertheit
- Unter Risiko wird die Gefahr verstanden, dass Ereignisse oder Handlungen im hindern, die anvisierten Ziele zu erreichen.
- Ziel des Risikomanagements ist es, alle Risiken (organisatorisch & technisch) adäquat erfassen, analysieren und bewerten. Ihre Veränderung zu dokumentieren und Gegenmaßnahmen durch festgelegten Risikostrategien einleiten
- Beachtung der rechtlichen und regulatorischen Anforderungen

05 Grundlagen Risikomanagement

- Aufstellung einer Risikoliste aus internen und externen Informationen
- Identifikation von
  - Assets
  - Bedrohungen
  - Schwachstellen
- Analyse von Ursachen, Quellen und Auswirkungen von Risiken in einer Risikoinventur (Schadensausmaß und Eintrittswahrscheinlichkeit)
- Festlegung der Eintrittswahrscheinlichkeiten oder Häufigkeiten und Schadenshöhe

05 Grundlagen Risikomanagement

- Identifikation von Möglichkeiten
  - Risikoreduktion
  - Klassische Sicherheitsmaßnahmen
  - Risikovermeidung
  - Risikotransfer
  - Risikoakzeptanz
- Bewertung, wie weit die ausgewählten Maßnahmen Risiken reduzieren
- Bestimmung des verbleibenden Risikos
- Managemententscheidung – formal, schriftlich, mit Begründung

06 ISMS

06 Information Security Management System

Eigenschaften und Ziele eines ISMS

- Verankerung in der Organisation
- Verbindliche Ziele
- Richtlinien
- Personalmanagement
- Aktualität des Wissens
- Qualifikation und Fortbildung
- Adaptive Sicherheit
- Vorbereitung

06 Information Security Management System

Grundlagen zur Einrichtung eines solchen Systems

- Grundschutz Kompendium
- BSI – Standards
- ISO´s
- ISIS 12 für KMU

07 ISO 27x

- *ISO 2700x*
- *ISO 27701*
- *ISIS 12*

07 ISO 2700x

International Organization for Standardization

- ISO 27000 Normen stellen eine Zertifizierungsgrundlage dar
- ISO 2700x
- ISO 27701

07 ISO 2700x

International Organization for Standardization

- ISO/IEC 27000 enthält Begriffe und Definitionen, welche in der Normenserie ISO/IEC 27000 verwendet werden.
- ISO/IEC 27001 enthält die Anforderungen an ein ISMS.
- ISO/IEC 27002 enthält Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit.
- Am 15. Juni 2005 wurde der Leitfaden ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management veröffentlicht, der auf BS 7799-1-Norm fußt. Bezugnehmend auf ISO/IEC JTC 1/SC 27 N5981 Secretariat ISO/IEC JTC 1/SC 27 – Deutsches Institut für Normung e.V. ist die Norm seit Sommer 2007 von ISO/IEC 17799:2005 in ISO/IEC 27002:2005 umbenannt worden.
- ISO/IEC 27003 enthält einen Leitfaden zur Umsetzung der ISO/IEC 27001 (herausgegeben im Februar 2010).
- ISO FCD 27004 „Information Security Management Measurement“ (herausgegeben im September 2012).
- ISO FCD 27005 ist an den BS 7799-3:2006 angelehnt und behandelt das Thema IS Risikomanagement (herausgegeben im Juni 2008).

07 ISO 27701

International Organization for Standardization

- Mit der neuen Norm **ISO/IEC 27701 (2019)** wird das klassische Informationssicherheitsmanagementsystem **ISO 27001** um Datenschutzaspekte erweitert, so dass beide Beauftragte über das gleiche Dokumentenwerk gegenseitig zuarbeiten können
- Informationssicherheitsbeauftragter und Datenschutzbeauftragter orientieren sich an gleichen Standards
- **Privacy Information Managementsystem (PIMS)**

07 ISIS12

Informationssicherheit für den Mittelstand

- ISIS12 ist ein Modell zur Einführung eines ISMS in kleinere und mittlere IT Infrastrukturen, um auch dort die systematische und kontinuierliche Informationssicherheit zu erhöhen.
- Abgeleitet und entwickelt aus dem Grundschutz-Kompendium und der ISO 27001, ist ISIS12 eine unabhängig zertifizierbare Einstiegsstufe und stellt die Grundlage dar, für eine umfangreichere Zertifizierung, z.B. gemäß ISO 27001, als Basis zu dienen.
- Entwickelt durch das Netz für Informationssicherheit im Mittelstand (NIM), war vordergründig, ein Einführungskonzept in verständlicher Sprache zu erstellen, welches es kleinen und mittleren Unternehmen ohne große IT Abteilung ebenfalls ermöglicht, der Informationssicherheit und natürlich auch gesetzlichen Vorgaben zu entsprechen.

07 ISIS12

Informationssicherheit für den Mittelstand

1. Leitlinie erstellen
2. Mitarbeiter sensibilisieren
3. Informationssicherheitsteam aufbauen
4. IT-Dokumentationsstruktur festlegen
5. IT-Servicemanagement-Prozess einführen
6. Kritische Applikationen identifizieren
7. IT-Struktur analysieren
8. Sicherheitsmaßnahmen modellieren
9. Ist-Soll vergleichen
10. Umsetzung planen
11. Umsetzen
12. Revision

VIELEN DANK!

Quellen

- Grafiken:
- https://storyset.com