BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

Datenschutz und Kryptographie

Modul DSKRY-40 im Studiengang Informatik

Referent: Dr. Hendrik Siegmund

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Quasi-Standard der Schutzmaßnahmen für Daten und Informationen
  - Grundgedanken und Modell
  - Begriffe
  - Komponenten
  - Methodik
  - Anwendungsbeispiele

Grafiken: Bundesamt für Sicherheit in der Informationstechnik

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Grundgedanken und Modell
- Axiome:
  - Informationen in IT-Systemen unterliegen verschiedenen Bedrohungen
  - In IT-Systemen gibt es stets verschiedene Schwachstellen
  - Trifft eine Bedrohung auf eine passende Schwachstelle, entsteht eine konkrete Gefährdung für Daten und Informationen

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Grundgedanken und Modell

Bedrohung + Schwachstelle = **Gefährdung**

Bild: Katholisches Datenschutzzentrum

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Grundgedanken und Modell
  - Bedrohungen sind allgegenwärtig und unvermeidbar
  - Schwachstellen können durch geeignete Maßnahmen eliminiert werden
  - Wird durch eine geeignete Maßnahme eine Schwachstelle beseitigt, so gilt die aus spezifischer Bedrohung und Schwachstelle entstehende Gefährdung ebenfalls als beseitigt, mindestens jedoch stark abgemildert.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Grundgedanken und Modell

Maßnahme

Bedrohung + Schwachstelle = ~~Gefährdung~~

Bild: Katholisches Datenschutzzentrum

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Grundgedanken und Modell
  - Bedrohungen und Schwachstellen sind variabel
  - Maßnahmen müssen sich kontinuierlich verändern
  - Der Aufwand ist dem Schutzbedarf der IT-Systeme, Daten und Informationen anzupassen

Unternehmensführung übernimmt Verantwortung und Initiative

Gefährdungen erkennen und bewerten

Angemessene Maßnahmen nach Stand der Technik ergreifen

Maßnahmen regelmäßig überprüfen und korrigieren

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
  - Unternehmensführung übernimmt Verantwortung und Initiative
  - Gefährdungen erkennen und bewerten
  - Angemessene Maßnahmen nach Stand der Technik ergreifen
  - Maßnahmen regelmäßig überprüfen und korrigieren

  - Mit diesen Aufgaben ist die Informationssicherheit handhabbar.
  - Daraus ergibt sich das Informationssicherheitsmanagementsystem ISMS

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

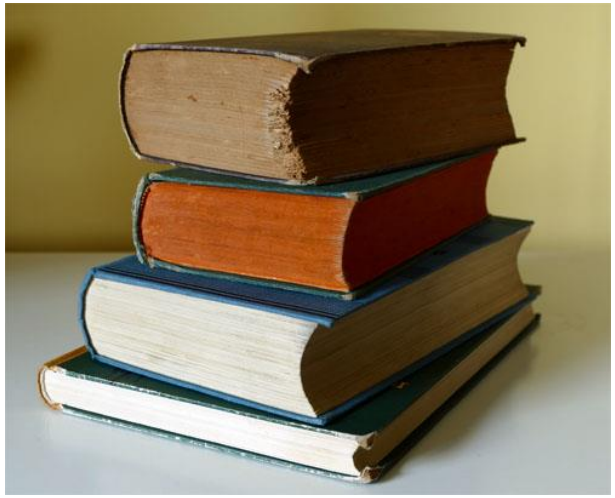
IT-Sicherheit

Quelle: BSI

- IT-Sicherheit – BSI Grundschutz

- Der BSI-Grundschutz behandelt den Aufbau und Betrieb eines Informationssicherheitsmanagementsystem ISMS
- Mit dem ISMS sollen IT-Sicherheit und Informationssicherheit etabliert und aufrecht erhalten werden.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION



IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Eigentlich ganz einfach – warum dann Hunderte von Seiten Umfang?
  - Vielfältige Bedrohungen
  - Vielfältige Schwachstellen
  - Komplexes System aus verschiedensten Maßnahmen auf technischer und organisatorischer Ebene: Prozesse und Systeme
  - Unterschiedlichste Vorgehensweisen für verschiedene Anwendungsfälle
  - Laufender Anpassungsbedarf, Informationssicherheitsmanagementsystem
  - Viele, nicht immer einheitlich verwendete Begriffe

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Bild: Pixabay

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Bedrohung (engl. Threat):
    - „Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann.“
    - Höhere Gewalt, technisches Versagen, menschliche Fehlhandlungen, vorsätzliche Handlungen

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Grafik: BrianAJackson/iStockphoto

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Schwachstelle (engl. Vulnerability):
    - „Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution.“
    - Ursachen liegen in Konzept, Software, Konfiguration, Betrieb oder Organisation

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Gefährdung (engl. Applied threat):
    - „Ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt.“
    - Im Grundschutz synonym mit Gefahr verwendet. Oft als konkrete Variante einer allgemeiner gefassten Gefahr verstanden. Beispiel: Gefahr ist die Offenlegung von Daten, verschiedene Gefährdungen können Diebstahl eines Datenträgers, Angriff auf Server oder unbefugtes Kopieren sein.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Quelle: datenschutzbeauftragter-info.de

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Angriff (engl. Attack):
    - „Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen.“
    - Kann aus eigenen Interessen oder im Interesse Dritter erfolgen

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

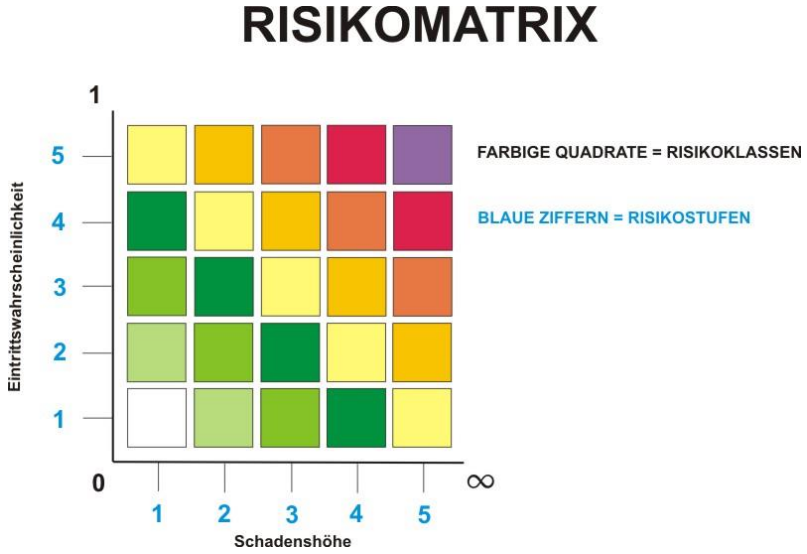
IT-Sicherheit

Quelle: medien.aktion-mensch.de

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Risiko:
    - Nach ISO 31000 „Auswirkung von Unwägbarkeiten auf Ziele“, sowohl negativ (Schaden) als auch positiv (Chance)
    - Hier aber: Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe
    - Bewertung der Relevanz eines gegebenen Schadenszenarios

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit



Quelle: Doeni, CreativeCommons.

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Risikoanalyse:
    - **Prozess** zur Beurteilung von Risiken aus den Schritten Identifizierung, Einschätzung/Analyse und Beurteilung.
    - Ergebnis ist ein bewertetes Risiko (Eintrittswahrscheinlichkeit, Schadenshöhe)
  - Risikoappetit:
    - Individuelle Neigung einer Institution zu Bewertung von bzw. Umgang mit Risiken

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Anforderung (im Grundschutz Synonym mit Sicherheitsanforderung):
    - Einzelne organisatorische, personelle, infrastrukturelle oder technische Maßnahme oder Maßnahmenkomplex zur Herbeiführung von Informationssicherheit
    - Im Grundschutz werden Anforderungen durch Bausteine erfüllt
    - Es wird zwischen Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf unterschieden

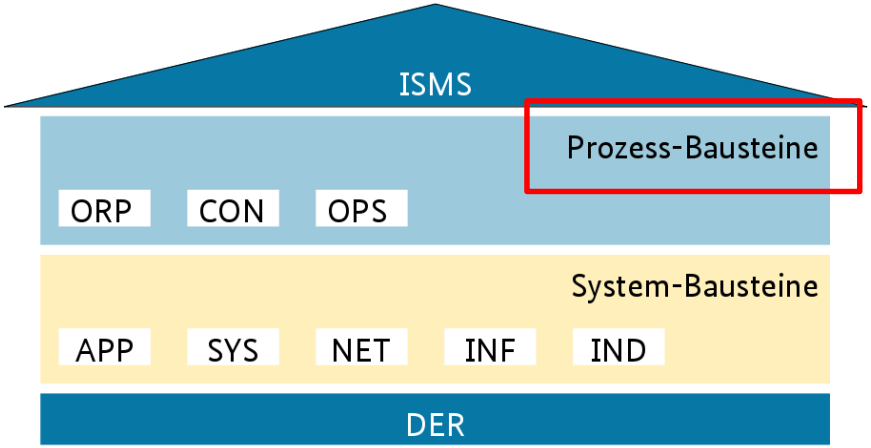
BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
  - Begriffe (vgl. Glossar im Grundschutz-Kompendium 2. Ed. 2019)
  - Bausteine
    - „Unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme, Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind.“
    - Bausteine machen das Grundschutzkonzept modular und universell einsetzbar
    - Unterscheidung in prozessorientierte und systemorientierte Bausteine

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit



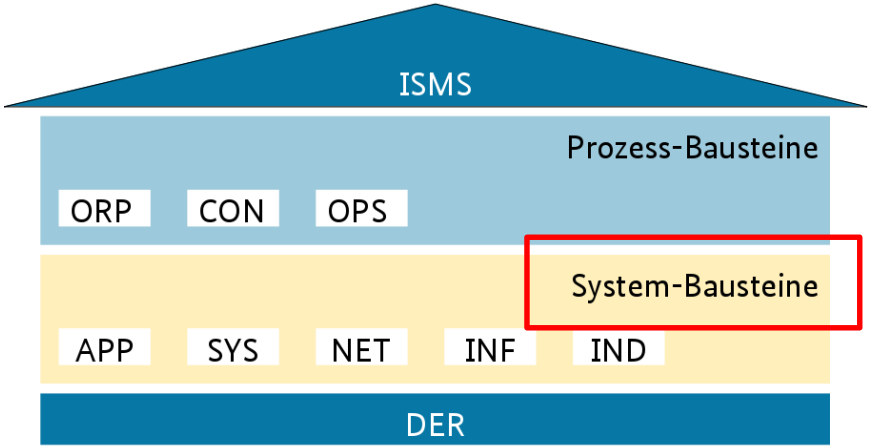
Quelle: BSI Grundschutz-Kompendium 2019

- IT-Sicherheit – BSI Grundschutz

- Komponenten 1: Bausteine
- Prozessbausteine (Organisatorisches, Konzepte, Vorgehensweisen)
  - ISMS (Sicherheitsmanagement)
  - ORP (Organisation und Personal)
  - CON (Konzepte und Vorgehensweisen)
  - OPS (Betrieb)
  - DER (Detektion & Reaktion)

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit



Quelle: BSI Grundschutz-Kompendium 2019

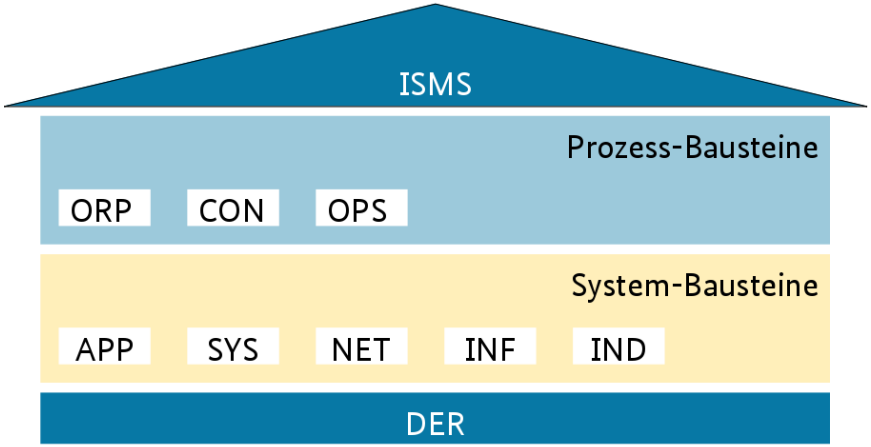
- IT-Sicherheit – BSI Grundschutz

- Komponenten 1: Bausteine
- Systembausteine (Technik)
  - APP (Anwendungen)
  - SYS (IT-Systeme)
  - IND (Industrielle IT)
  - NET (Netze und Kommunikation)
  - INF (Infrastruktur)

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine
- Einordnung im Schichtenmodell
  - Übergeordnetes Informations-sicherheitsmanagementsystem
  - Logische Ebene der Prozess-Bausteine
  - Logische Ebene der System-Bausteine
  - Detektion und Reaktion



Quelle: BSI Grundschutz-Kompendium 2019

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Beispiel:
- Prozessbaustein OPS (Betrieb)
- Drei Teilbausteine
  - OPS1, Kern-IT-Betrieb und weiterführende Aufgaben
  - OPS2, Betrieb von Dritten
  - OPS3, Betrieb für Dritte

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Prozessbaustein OPS (Betrieb)
  - OPS1, Kern-IT-Betrieb
    - OPS1.1.2 Ordnungsgemäße IT-Administration
    - OPS1.1.3 Patch- und Änderungsmanagement
    - OPS1.1.4 Schutz vor Schadprogrammen
    - OPS1.1.5 Protokollierung
    - OPS1.1.6 Software-Tests und -Freigaben

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Prozessbaustein OPS (Betrieb)
  - OPS1, Weiterführende Aufgaben
    - OPS1.2.2 Archivierung
    - OPS1.2.3 Informations- und Datenträgeraustausch
    - OPS1.2.4 Telearbeit

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Prozessbaustein OPS (Betrieb)
  - OPS2, Betrieb von Dritten
    - OPS2.1 Outsourcing für Kunden
    - OPS2.2 Cloud-Nutzung
    - OPS 2.4 Fernwartung
  - OPS3, Betrieb für Dritte
    - OPS3.1 Outsourcing für Dienstleister

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Beispiel:
- Systembaustein SYS (IT-Systeme)
- Vier Teilbausteine
  - SYS1, Server
  - SYS2, Desktop-Systeme
  - SYS3, Mobile Devices
  - SYS4, Sonstige Systeme

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Systembaustein SYS (IT-Systeme), Server
  - SYS1.1 Allgemeiner Server
  - SYS1.2 Windows Server 2012
  - SYS1.3 Server unter Unix
  - SYS1.5 Virtualisierung
  - SYS1.7 IBM Z-System
  - SYS1.8 Speicherlösungen

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Systembaustein SYS (IT-Systeme), Desktop-Systeme
  - SYS2.1 Allgemeiner Client
  - SYS2.2.2 Client unter Windows 8.1
  - SYS2.2.3 Client unter Windows 10
  - SYS2.3 Client unter Unix
  - SYS2.4 Client unter MacOS

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Systembaustein SYS (IT-Systeme), Mobile Devices
  - SYS3.1 Laptops
  - SYS3.2.1 Allgemeine Smartphones und Tablets
  - SYS3.2.2 Mobile Device Management
  - SYS3.2.3 iOS (for Enterprise)
  - SYS3.2.4 Android
  - SYS3.3 Mobiltelefon
  - SYS3.4 Mobile Datenträger

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine - Herausforderung große Vielzahl
- Systembaustein SYS (IT-Systeme), Sonstige Systeme
  - SYS4.1 Drucker, Kopierer, Multifunktionssysteme
  - SYS4.3 Eingebettete Systeme
  - SYS4.4 Allgemeines IoT-Gerät

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 1: Bausteine
- Für den Aufbau eines ISMS müssen alle in einer Organisation genutzten Bausteine mindestens einmal berücksichtigt werden.
- Nicht genutzte Bausteine des Grundschutz-Kompendiums brauchen nicht bearbeitet zu werden.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Quelle: Fairsicherungsladen-Freiburg

Quelle: spiegel.de

- IT-Sicherheit – BSI Grundschutz
- Komponenten 2: Gefährdungen
- Grundschutz-Kompendium nennt 47 Elementare Gefährdungen
  - G001 Feuer
  - …
  - G047 Schädliche Seiteneffekte IT-gestützter Angriffe

  - Beschreibung der elementaren Gefährdungen siehe Grundschutz-Kompendium 2. Ed. 2019, S. 74-121.
  - Ersetzt bisherige Gefahrenkataloge

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Quelle: esmog-shop.com

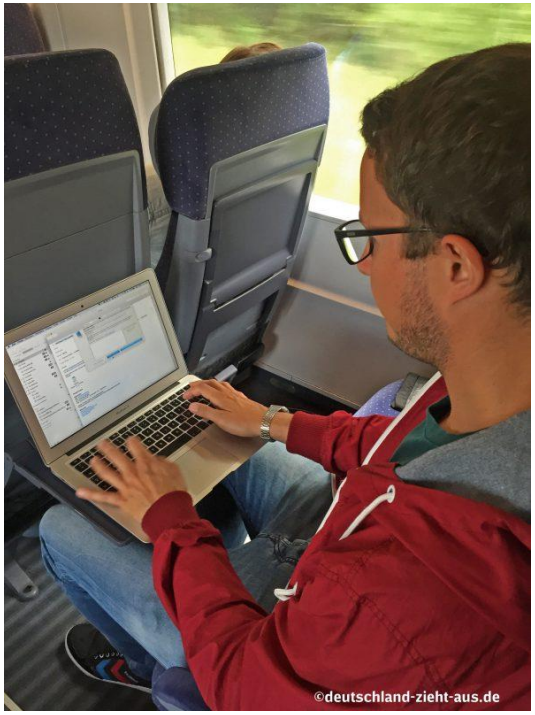
- IT-Sicherheit – BSI Grundschutz
- Komponenten 2: Gefährdungen – Beispiele
  - Allgemein bekannt sind G001 Feuer, G003 Wasser oder G005 Naturkatastrophen
  - Weniger bekannt ist G013 Abfangen kompromittierender Strahlung:
    - IT-Endgeräte und Netzwerke (nicht nur WLAN) senden elektromagnetische Strahlung aus, die Informationen enthalten und abgefangen werden kann.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Quelle: shop-alarm.de

- IT-Sicherheit – BSI Grundschutz
- Komponenten 2: Gefährdungen - Beispiele
  - G014 Ausspähen von Informationen (Spionage)
  - Oft äußerst sorgloser Umgang mit Informationen, z.B. Arbeit an vertraulichen Dokumenten in der Bahn
  - G 0.15 Abhören
  - Technik dafür im Handel frei erhältlich
  - Kundengespräche am Telefon in der Bahn



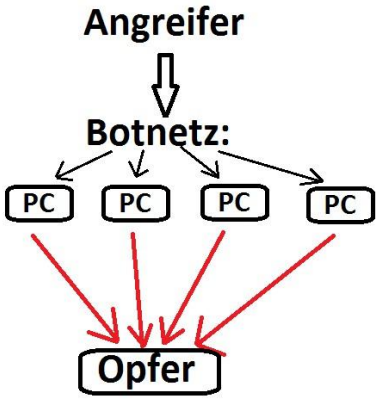
Quelle: inside-bahn.de

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Quelle: it-daily.net

- IT-Sicherheit – BSI Grundschutz
- Komponenten 2: Gefährdungen – Beispiele
  - G040 Verhinderung von Diensten (Denial of Service)
  - Meist gezielter Angriff auf ein System, um dieses durch Überlastung außer Betrieb zu setzen
  - Viele synchronisierte Angreifer
  - Bot-Netz infizierter PCs, Distributed DoS-Attacke



Quelle: praxistipps.chip.de

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Bild: drogatnev / iStock.com / Getty Images

- IT-Sicherheit – BSI Grundschutz
- Komponenten 2: Gefährdungen – Beispiele
  - G 0.42 Social Engineering
  - Versuch, durch soziale Interaktion an vertrauliche Informationen zu gelangen
    - Erschleichen von Zugangsdaten (Phishing) durch manipulierte E-Mails, z.B. „vom Chef“
    - Telefonanrufe mit gestellten „Notsituationen“
    - Installation

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Von: Hendrik Siegmund <hendrik@3gi.co.za>
Gesendet: [redacted]
An: [redacted]@diakonie-leipzig.de>
Betreff: IUK 1157621

Guten Morgen [redacted]

Im Anhang dieser E-Mail finden Sie eine .doc-Datei mit den gewünschten Informationen.

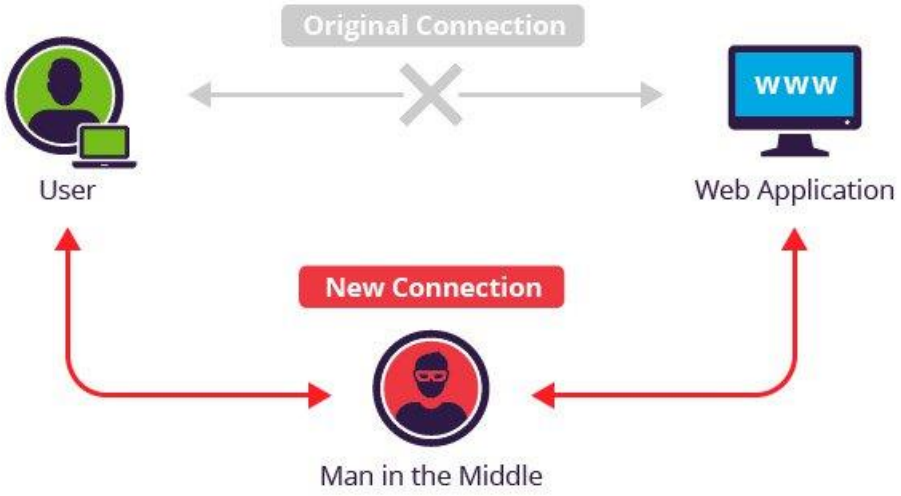
http://magistradossisidro.org.ar/Rechnung-Nr-87945/XMYRBTH9VL08/

Freundliche Grüße
Hendrik Siegmund

Mit freundlichen Grüßen
Dr. Hendrik Siegmund

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit



Quelle: imperva.com

- IT-Sicherheit – BSI Grundschutz
- Komponenten 2: Gefährdungen – Beispiele
  - G 0.43 Einspielen von Nachrichten
  - Replay-Attacke: Aufzeichnen und erneutes Verwenden einer Nachricht
  - Man-in-the-Middle-Attacke:
    - Kommunikation wird zwischen Absender und Empfänger abgefangen und unbemerkt unterbrochen.
    - Angreifer täuscht vor, der erwünschte Absender oder Empfänger zu sein und erhält so vertrauliche Informationen.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 3: Bausteine und Gefährdungen – Beziehungen
- Grundgedanke
  - Gefährdungen wirken z.B. auf einen Systembaustein
  - Prozessbausteine mildern die Gefährdungen ab oder beseitigen sie. Unzureichender Einsatz von Prozessbausteinen erhöht Gefährdungen
- Beispiel
  - G045 Datenverlust bedroht SYS1.1 Allgemeiner Server
  - CON.3.A5 Regelmäßige Datensicherung kann Datenverlust verhindern
  - Weitere Prozessbausteine für vollständige Gefahrenbeseitigung erforderlich

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 3: Bausteine und Gefährdungen - Beziehungen
  - Nicht alle Gefährdungen stehen mit allen Bausteinen in Beziehung
  - Welche Gefährdungen mit welchen Bausteinen in Beziehung stehen, wird durch Kreuzreferenztabellen definiert.

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 4: Kreuzreferenztabellen
- Funktionsweise
  - Für jeden Prozess- und Systembaustein eine Matrix aus allen Teilbausteinen und den hierfür bedeutsamen elementaren Gefährdungen
- Beispiel:
  - Gefährdungen, die sich auf die Teilprozesse einer Datensicherung auswirken können

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Elementare Gefährdungen Anforderungen	G 0.2	G 0.4	G 0.14	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.28	G 0.29	G 0.31	G 0.45	G 0.46
CON.3.A1			X		X		X			X		X	X
CON.3.A2				X									
CON.3.A3			X		X		X			X		X	X
CON.3.A4				X									
CON.3.A5				X		X							
CON.3.A6				X									
CON.3.A7										X			
CON.3.A8							X	X	X				
CON.3.A9				X			X	X			X	X	
CON.3.A10				X								X	X
CON.3.A11										X		X	
CON.3.A12	X	X				X	X					X	
CON.3.A13				X		X						X	

Kreuzreferenztabellen für CON 3 Datensicherung. Quelle: BSI Grundschutz-Kompendium 2. Ed. 2019

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Komponenten 4: Kreuzreferenztabellen
  - Kreuzreferenztabellen schließen den Kreis zum Grundgedanken:

Baustein(e)

El. Gefährdung + Schwachstelle = IT-Sicherheit

Bild: Katholisches Datenschutzzentrum

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Quasi-Standard zu Schutzmaßnahmen für Daten und Informationen
  - Grundgedanken und Modell
  - Begriffe
  - Komponenten
  - Methodik
  - Anwendungsbeispiele

Grafiken: Bundesamt für Sicherheit in der Informationstechnik

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Übersicht – Idee und Bausteine
- Grundidee: **Bausteine** gegen **Gefährdungen** schaffen **IT-Sicherheit**
  - Bausteine für operatives Handeln: **Prozessbausteine**
    - ISMS, OPR, CON, OPS, DER
  - Bausteine für Technikbetrieb: **Systembausteine**
    - APP, SYS, NET, IND, INF
  - Die Bausteine bieten **Handlungsempfehlungen**

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Übersicht – Modalverben
  - Handlungsempfehlungen nutzen **Modalverben** MUSS und SOLLTE sowie entsprechende Negationen:
    - MUSS / DARF NUR
    - DARF NICHT / DARF KEIN

    } **Zwingend** zu tun/ zu unterlassen

    - SOLLTE
    - SOLLTE NICHT / /SOLLTE KEIN

    } **Normalerweise** zu tun/ zu unterlassen

    - Umsetzung wird bei Audits geprüft!

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Übersicht – Rollen
- An Rollen werden Verantwortlichkeiten bzw. Zuständigkeiten für die Umsetzung von/in Bausteinen geknüpft, z.B.
  - **Institutionsleitung**: Oberste Leitungsebene, Verantwortung für IT-Sicherheit
  - **Informationssicherheitsbeauftragter** (ISB): Unterstützt und berät Leitungsebene
  - **Fachverantwortliche**: Abteilungsleitung, Verantwortlich für Fachverfahren
  - **Leiter IT**: Verantwortlich für IT-Betrieb etc.
  - **Administrator**: Betreut ein oder mehrere IT-System(e)
  - **Benutzer**: Mitarbeitende mit IT-Systemzugang

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Aktuelle Dokumente
  - BSI-IT-Grundschutzkompendium: Einführung und Erläuterung
  - BSI-Standard 200-1: Informationssicherheitsmanagementsysteme
  - BSI-Standard 200-2: IT-Grundschutz-Methodik
  - BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - BSI-Standard 100-4: Notfallmanagement
  - Leitfaden zur Basis-Absicherung: Grundschutz „light“ für KMU

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

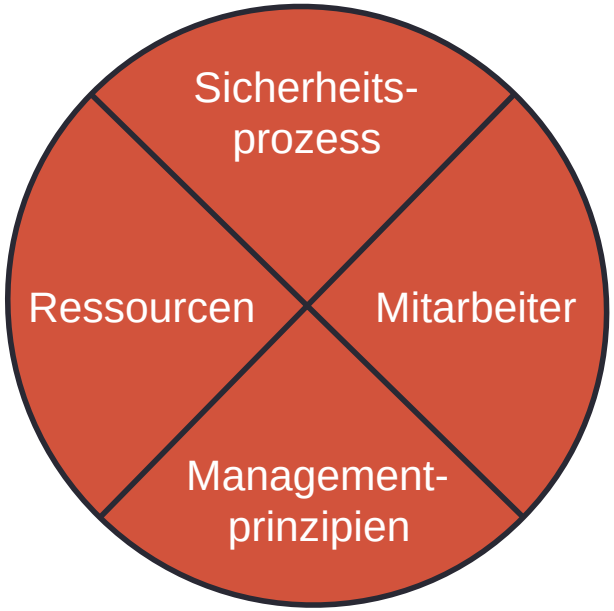
IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Vorgehensweise (BSI-Standard 200-1 und 200-2)
  - Ein Managementsystem für Informationssicherheit (ISMS) ist aufzubauen
  - Das ISMS hat mehrere Bestandteile
  - Der Weg zum ISMS und dessen Betrieb wird als Prozess verstanden: Sicherheitsprozess
  - Der Sicherheitsprozess hat mehrere Phasen und Schritte
  - Einige Schritte sind nach Etablieren des ISMS regelmäßig zu wiederholen

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – Bestandteile
  - Sicherheitsprozess
    - Informationssicherheitsleitlinie (Sicherheitsziele, Umsetzungsstrategie)
    - Sicherheitsorganisation
    - **Sicherheitskonzept**
  - Ressourcen
  - Mitarbeiter
  - Managementprinzipien
    - Regeln und Richtlinien



BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
LEIPZIG
UNIVERSITY OF COOPERATIVE EDUCATION

IT-Sicherheit

Fragen zum Selbststudium

- Welche Grundgedanken und welches einfache Modell steht hinter dem BSI-Grundschutzkonzept?
- Wer ist nach BSI-Grundschutz für den Aufbau eines ISMS verantwortlich?
- Was verstehen Sie im Grundschutz-Zusammenhang unter den Begriffen Bedrohung, Schwachstelle und Gefährdung
- In welche zwei Gruppen teilt der Grundschutz seine Bausteine ein? Zu welchen Gruppen gehören a) Windows Server und b) Datensicherung?
- Was wird in einer Kreuzreferenztabelle dargestellt?

Quellen: Dieses Skript, BSI-Grundschutz-Kompendium unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html