

IT-Grundschutz

Fundament und Arbeitswerkzeug für ganzheitliche Informationssicherheit

3. IT-Grundschutz-Tag 2023 – 13.04.2023

Christoph Wiemers– Referat BSI-Standards und IT-Grundschutz

Einstieg und Motivation



Informationssicherheit



- Informationssicherheit hat den Schutz von Informationen als Ziel
- Grundwerte der Informationssicherheit sind dabei u.a. die **Verfügbarkeit, Vertraulichkeit und Integrität** von Informationen
- Informationen können dabei auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein

Informationssicherheit liefert mehr als reine IT-Sicherheit

Informationssicherheit



...ist kein Produkt!

- Sicherheit kann man nicht kaufen
- Sicherheit muss man schaffen
- Natürlich kann man dazu auch auf vorhandene Produkte zurückgreifen

...ist kein Projekt!

- Es genügt nicht, Sicherheit einmal zu schaffen
- Sicherheit muss aufrechterhalten werden

... ist ein Prozess und Chefsache!

Informationssicherheit



Wir haben doch schon was getan! Wirksamkeit? Angemessenheit?



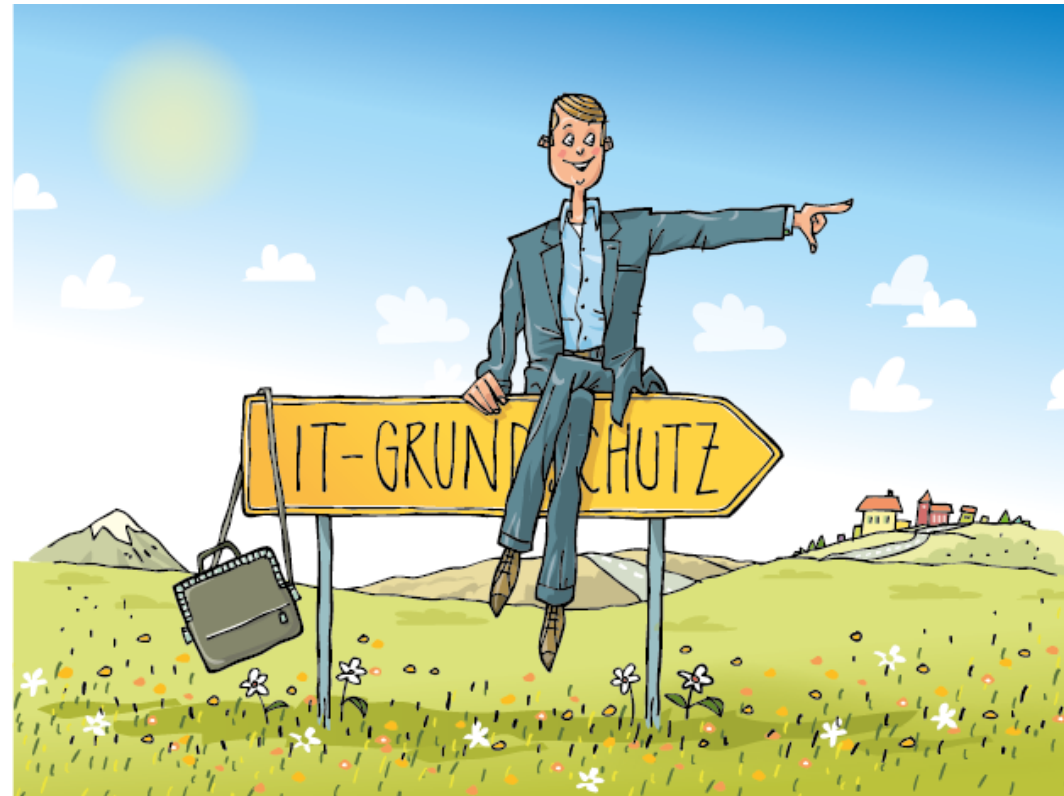
Informationssicherheit etablieren

- Zur Schaffung von Informationssicherheit ist es nicht ausreichend, einmalig ein **statisches** Sicherheitskonzept zu erstellen
- Statische Sicherheitskonzepte können durch das **dynamische Umfeld** mit sich ständig verändernder Bedrohungslage, neuen Angriffsvektoren usw. eine **andauernde Informationssicherheit** nicht wirksam gewährleisten
- Der Schlüssel zu einem **angemessenen Schutz** von Geschäftsprozessen/Informationen ist ein **systematisches Vorgehen** → Etablierung eines **Managementsystems für Informationssicherheit (ISMS)**
- ISMS bezeichnet die Planungs-, Lenkungs- und Kontrollaufgabe zu Aufbau, Aufrechterhaltung und kontinuierlicher Verbesserung eines durchdachten und wirksamen **Sicherheitsprozesses**

Viele Wege führen zu einem ISMS



...welcher Weg ist
der effektivste?



Managementsystem für Informationssicherheit (ISMS)



- Ein ISMS beinhaltet diverse Aspekte, die in der **IT-Grundschutz-Methodik** berücksichtigt werden
- Die **BSI-Standards** und das **IT-Grundschutz-Kompendium** bilden die Hauptwerke im IT-Grundschutz

BSI-Standards

- Die **BSI-Standards** 200-1 bis 200-3 erläutern, wie ein ISMS in einer Institution aufgebaut werden kann und die in den Geschäftsprozesse bzw. Fachaufgaben verarbeiteten Informationen abgesichert werden können



IT-Grundschutz-Kompodium



- Im **IT-Grundschutz-Kompodium** beschreiben Fachtexte, die sogenannten IT-Grundschutz-Bausteine, was ein Anwender tun muss, um einen bestimmten Bereich abzusichern
- Dabei wird ein ganzheitlicher Ansatz verfolgt: Infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsanforderungen helfen, ein **Standard-Sicherheitsniveau** aufzubauen, um geschäftsrelevante Informationen zu schützen
- An vielen Stellen werden bereits höherwertige Sicherheitsanforderungen geliefert, die die Basis für sensiblere Bereiche sind



Effiziente Vorgehensweise



- Klassische Vorgehensweisen für den Aufbau eines ISMS, z. B. ISO 27001, führen zu Beginn für den gesamten Geltungsbereich umfangreiche und zeitintensive **Risikoanalysen** durch
- Risiken werden ermittelt und Eintrittswahrscheinlichkeiten/Schadenauswirkungen abgeschätzt, um daraus angemessene **Sicherheitsmaßnahmen** zu **erarbeiten**
- Mit IT-Grundschutz **entfällt** bei normalem Schutzbedarf und typischen Einsatzszenarien der **Aufwand** für die Risikoanalysen und Erarbeitung von Sicherheitsanforderungen bzw. Sicherheitsmaßnahmen
- Der Vorteil für die Anwender ist ein deutlich reduzierter Aufwand, da direkt mit der **Umsetzung der Anforderungen** aus dem IT-Grundschutz-Kompendium begonnen werden kann



Verlässlicher Indikator für Informationssicherheit

- Ein ISMS nach ISO 27001 erfüllt die **selbst** von der Institution **gesetzten Sicherheitsziele**, es wird **kein** definiertes **Sicherheitsniveau vorgegeben**
- Durch weniger konkrete Vorgaben besteht mehr Spielraum bei der Implementierung bis hin zur Akzeptanz von Risiken und zum Auslassen der Umsetzung von Maßnahmen (Controls Annex A), somit ist eine **Vergleichbarkeit** zwischen ISO 27001 Umsetzungen nur **schwer gegeben**
- IT-Grundschutz gibt ein **konkret definiertes Sicherheitsniveau** vor, das **nicht unterschritten** werden darf
- Dadurch ist eine **Vergleichbarkeit** gegeben, die als **verlässlicher Indikator** bei der Kooperation verschiedener Institutionen dient

Das IT-Grundschutz-Kompendium und die BSI-Standards

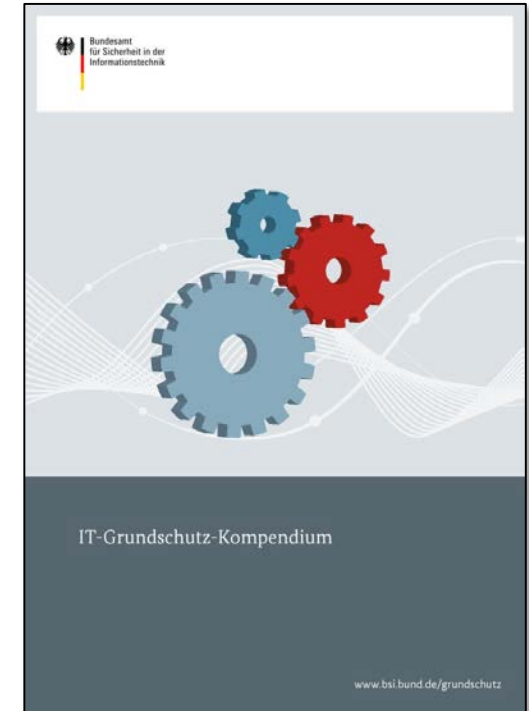


IT-Grundschutz-Kompendium Edition 2023



Bausteine

- 111 Bausteine
- Online in verschiedenen Formaten (Details nächste Folie)
- Druckversion beim Reguvis Verlag bestellbar





Auszug von Schichten und Bausteinen

ISMS: Sicherheitsmanagement

- ↳ ISMS.1 Sicherheitsmanagement

ORP: Organisation und Personal

- ↳ ORP.1 Organisation
- ↳ ORP.2 Personal
- ↳ ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ↳ ORP.4 Identitäts- und Berechtigungsmanagement
- ↳ ORP.5 Compliance Management (Anforderungsmanagement)

CON: Konzeption und Vorgehensweise

- ↳ CON.1 Kryptokonzept
- ↳ CON.2 Datenschutz
- ↳ CON.3 Datensicherungskonzept
- ↳ CON.6 Löschen und Vernichten
- ↳ CON.7 Informationssicherheit auf Auslandsreisen
- ↳ CON.8 Software-Entwicklung
- ↳ CON.9 Informationsaustausch
- ↳ CON.10 Entwicklung von Webanwendungen
- ↳ CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

OPS: Betrieb

- ↳ OPS.1.1.1 Allgemeiner IT-Betrieb
- ↳ OPS.1.1.2 Ordnungsgemäße IT-Administration
- ↳ OPS.1.1.3 Patch- und Änderungsmanagement
- ↳ OPS.1.1.4 Schutz vor Schadprogrammen
- ↳ OPS.1.1.5 Protokollierung
- ↳ OPS.1.1.6 Software-Tests und -Freigaben
- ↳ OPS.1.1.7 Systemmanagement
- ↳ OPS.1.2.2 Archivierung
- ↳ OPS.1.2.4 Telearbeit
- ↳ OPS.1.2.5 Fernwartung
- ↳ OPS.1.2.6 NTP -Zeitsynchronisation
- ↳ OPS.2.2 Cloud-Nutzung
- ↳ OPS.2.3 Nutzung von Outsourcing
- ↳ OPS.3.2 Anbieten von Outsourcing

DER: Detektion und Reaktion

- ↳ DER.1 Detektion von sicherheitsrelevanten Ereignissen
- ↳ DER.2.1 Behandlung von Sicherheitsvorfällen
- ↳ DER.2.2 Vorsorge für die IT-Forensik
- ↳ DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
- ↳ DER.3.1 Audits und Revisionen
- ↳ DER.3.2 Revision auf Basis des Leitfadens IS-Revision
- ↳ DER.4 Notfallmanagement

APP: Anwendungen

- ↳ APP.1.1 Office-Produkte
- ↳ APP.1.2 Webbrowser
- ↳ APP.1.4 Mobile Anwendung (Apps)
- ↳ APP.2.1 Allgemeiner Verzeichnisdienst
- ↳ APP.2.2 Active Directory Domain Services
- ↳ APP.2.3 OpenLDAP
- ↳ APP.3.1 Webanwendungen und Webservices
- ↳ APP.3.2 Webserver
- ↳ APP.3.3 Fileserver
- ↳ APP.3.4 Samba
- ↳ APP.3.6 DNS-Server
- ↳ APP.4.2 SAP-ERP-System
- ↳ APP.4.3 Relationale Datenbanksysteme
- ↳ APP.4.4 Kubernetes
- ↳ APP.4.6 SAP ABAP-Programmierung
- ↳ APP.5.2 Microsoft Exchange und Outlook
- ↳ APP.5.3 Allgemeiner E-Mail-Client und -Server
- ↳ APP.5.4 Unified Communications and Collaboration
- ↳ APP.6 Allgemeine Software
- ↳ APP.7 Entwicklung von Individualsoftware

SYS: IT-Systeme

- ↳ SYS.1.1 Allgemeiner Server
- ↳ SYS.1.2.2 Windows Server 2012
- ↳ SYS.1.2.3 Windows Server
- ↳ SYS.1.3 Server unter Linux und Unix
- ↳ SYS.1.5 Virtualisierung
- ↳ SYS.1.6 Containerisierung
- ↳ SYS.1.7 IBM Z
- ↳ SYS.1.8 Speicherlösungen
- ↳ SYS.1.9 Terminalserver

NET: Netze und Kommunikation

- ↳ NET.1.1 Netzarchitektur und -design
- ↳ NET.1.2 Netzmanagement
- ↳ NET.2.1 WLAN-Betrieb
- ↳ NET.2.2 WLAN-Nutzung
- ↳ NET.3.1 Router und Switches
- ↳ NET.3.2 Firewall
- ↳ NET.3.3 VPN
- ↳ NET.3.4 Network Access Control
- ↳ NET.4.1 TK-Anlagen
- ↳ NET.4.2 VoIP
- ↳ NET.4.3 Faxgeräte und Faxserver

INF: Infrastruktur

- ↳ INF.1 Allgemeines Gebäude
- ↳ INF.2 Rechenzentrum sowie Serverraum
- ↳ INF.5 Raum sowie Schrank für technische Infrastruktur
- ↳ INF.6 Datenträgerarchiv
- ↳ INF.7 Büroarbeitsplatz
- ↳ INF.8 Häuslicher Arbeitsplatz
- ↳ INF.9 Mobiler Arbeitsplatz
- ↳ INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum
- ↳ INF.11 Allgemeines Fahrzeug
- ↳ INF.12 Verkabelung
- ↳ INF.13 Technisches Gebäudemanagement
- ↳ INF.14 Gebäudeautomation



Bausteine

- Umfang: ca. 10 Seiten!
- Bestehen aus Einleitung, Zielsetzung, Abgrenzung und Modellierung, spezifische Gefährdungslage und Anforderungen
- Basis-Anforderungen, Standard-Anforderungen und Anforderungen für den erhöhten Schutzbedarf
- Die Anforderungen geben vor, was getan werden muss, um einen bestimmten Bereich abzusichern



BSI-Standards – Methode und Anleitung



- Inhalt
 - 200-1: **Managementsysteme für Informationssicherheit**
 - 200-2: **IT-Grundschutz-Methodik**
 - 200-3: **Risikoanalyse auf der Basis von IT-Grundschutz**
 - 200-4: **Business Continuity Management** (~~CD-Phase~~)
- Verfügbare Versionen
 - Kostenlos als PDF auf BSI-Webseite
 - Kostenpflichtige gedruckte Version über Reguvis Fachmedien GmbH (ehemals Bundesanzeiger Verlag)

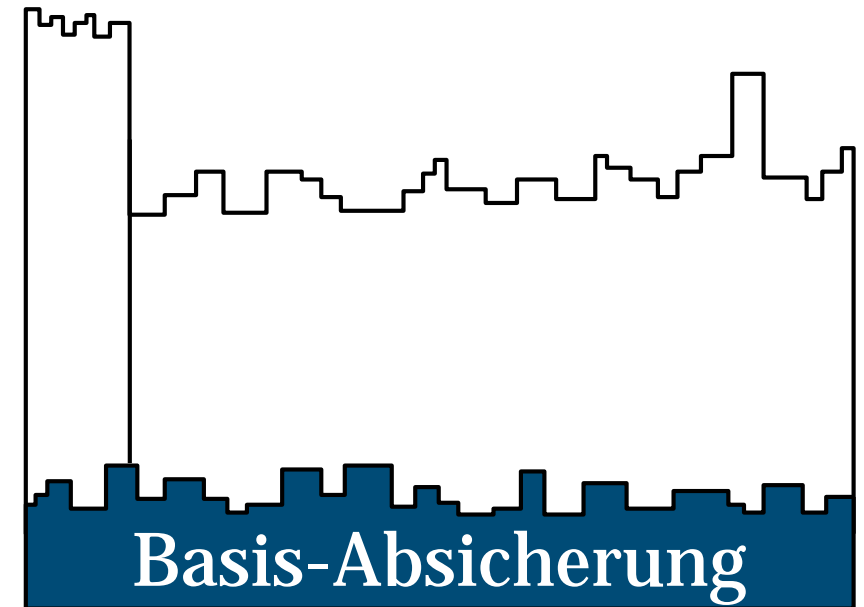


Überblick über die Vorgehensweisen



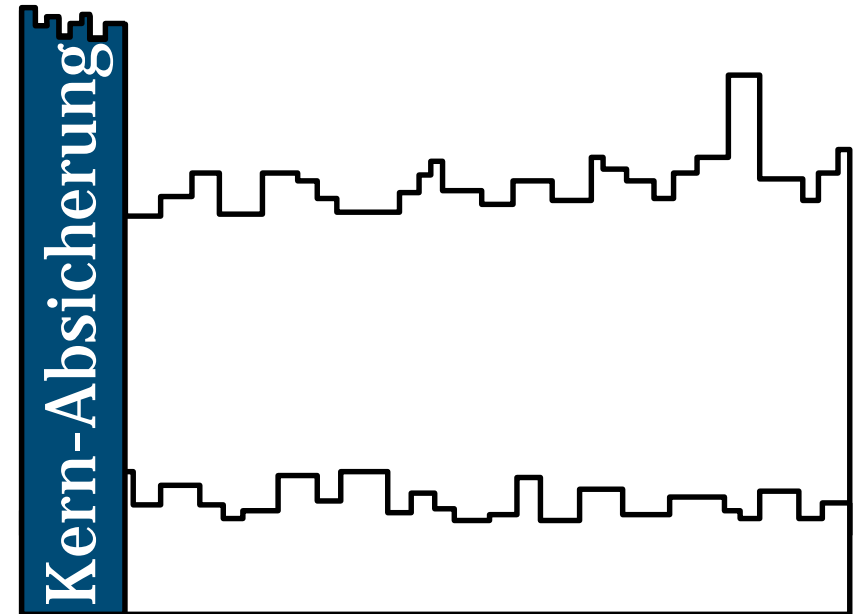
Basis-Absicherung

- **Vereinfachter Einstieg** in das Sicherheitsmanagement
- Grundlegende **Erstabsicherung** der Geschäftsprozesse und Ressourcen
 - Erstabsicherung in der Breite
 - Umsetzung essentieller Anforderungen
- Auf die Bedürfnisse von **KMUs** zugeschnitten
- Auch für **kleine Institutionen** geeignet



Kern-Absicherung

- Schutz herausragender, besonders gefährdeter Geschäftsprozesse und Ressourcen (**Kronjuwelen**)
- Unterschied zu IT-Grundschutz Classic: Fokussierung auf einen kleinen, aber **sehr wichtigen Informationsverbund**
- **Zeitersparnis** im Vorgehen
- **beschleunigte Absicherung** dieser Ressourcen in der Tiefe



Standard-Absicherung

- Implementierung eines **vollumfänglichen** Sicherheitsprozesses (kompatibel zur ISO 27001)
- Zertifizierbar **nach ISO 27001 auf der Basis von IT-Grundschutz**





Vorgehen nach IT-Grundschutz*

Strukturanalyse

Schutzbedarfsfeststellung

Modellierung

IT-Grundschutz-Check

Risikoanalyse

- Erfassung der Bestandteile des Informationsverbundes (Geltungsbereichs) ausgehend von **Geschäftsprozessen, Anwendungen, IT-Systemen/-Komponenten, Räumen** und **Gebäuden**
- Die einzelnen „Objekte“ werden **Zielobjekte** genannt
- Gruppierungen möglich

*Kern-/Standard-Absicherung, nur Teile bei Basis-Absicherung



Vorgehen nach IT-Grundschutz

Strukturanalyse

Schutzbedarfsfeststellung

Modellierung

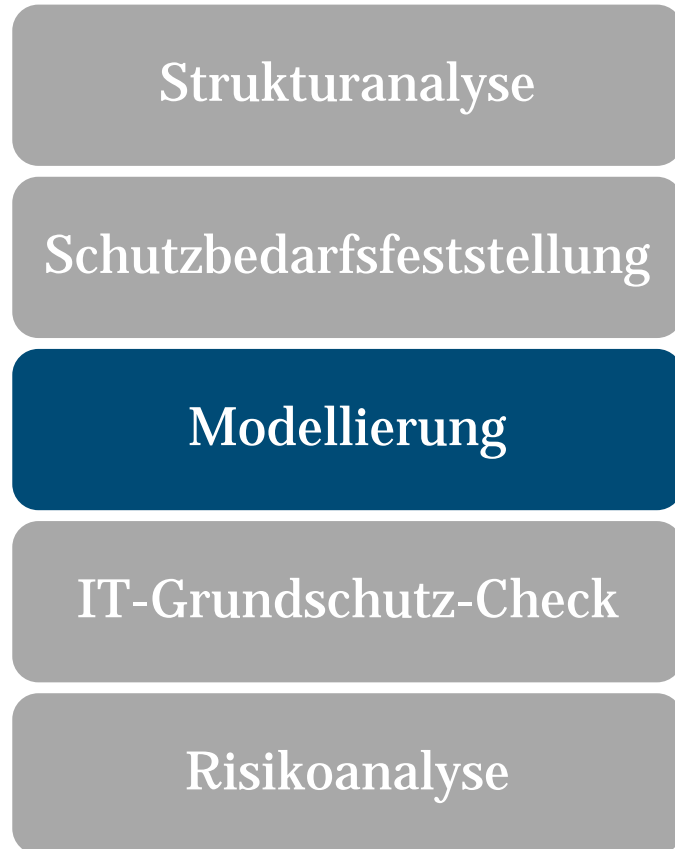
IT-Grundschutz-Check

Risikoanalyse

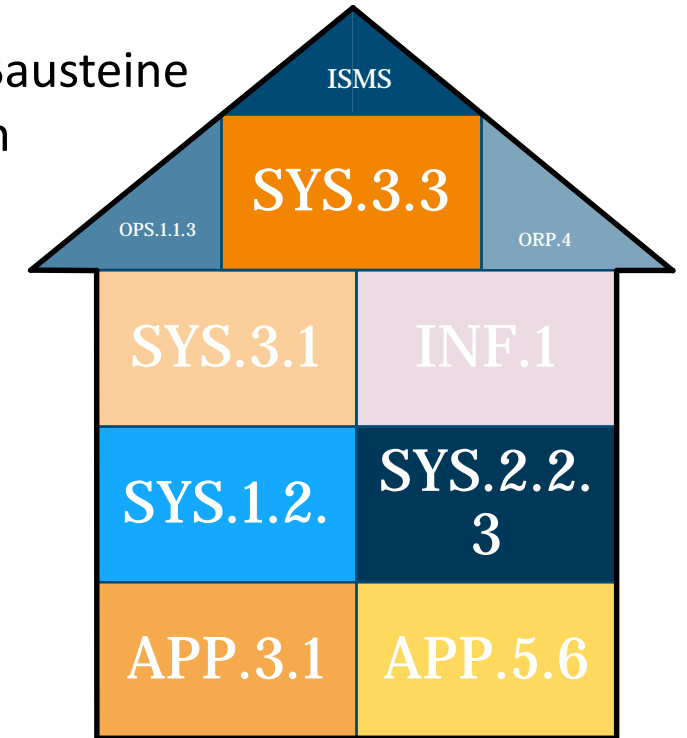
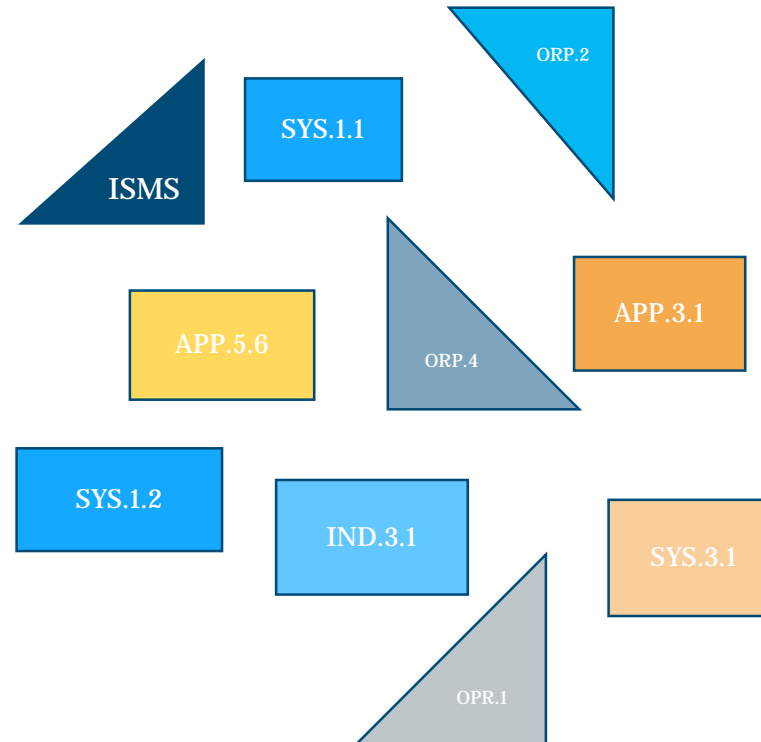
- Bestimmung des **Schutzbedarfs** für alle Zielobjekte aus der Strukturanalyse bezüglich **Vertraulichkeit, Integrität** und **Verfügbarkeit**
- Der Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Geschäftsprozesse und der damit verbundenen Anwendungen eintreten können
- Anschließend wird daraus der Schutzbedarf für alle weiteren Zielobjekte (z. B. IT-Systeme, Räume, Kommunikationsverbindungen) **abgeleitet**



Vorgehen nach IT-Grundschutz



- **Nachbildung** (Modellierung) des Informationsverbundes mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium





Vorgehen nach IT-Grundschutz

Strukturanalyse

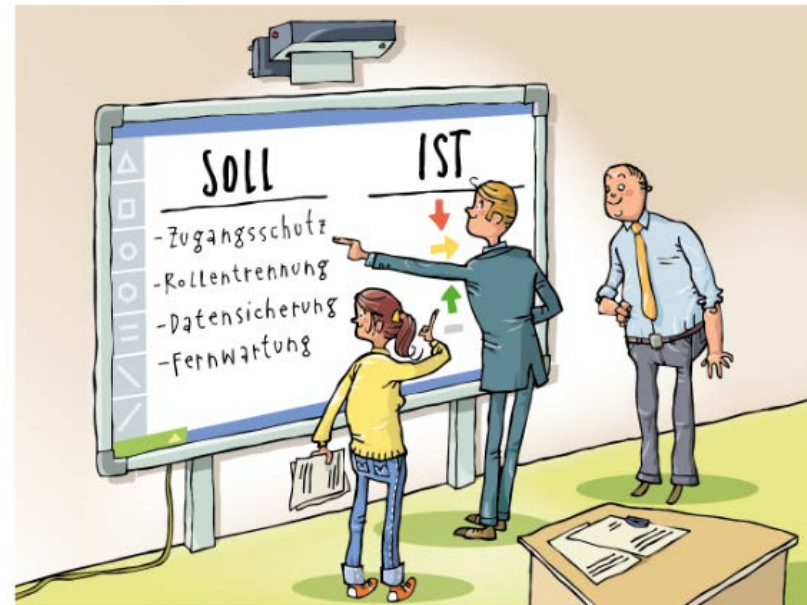
Schutzbedarfsfeststellung

Modellierung

IT-Grundschutz-Check

Risikoanalyse

- Soll/Ist-Vergleich
- Welche **Anforderungen** aus dem IT-Grundschutz-Kompendium sind bereits **umgesetzt** und welche müssen noch umgesetzt werden?





Vorgehen nach IT-Grundschutz

Strukturanalyse

Schutzbedarfsfeststellung

Modellierung

IT-Grundschutz-Check

Risikoanalyse

- Bei normalem Schutzbedarf und typischen Einsatzszenarien ist **keine** Risikoanalyse notwendig
- Bei
 - **hohem** oder **sehr hohem Schutzbedarf** oder
 - wenn **besondere Einsatzbedingungen** vorliegen oder
 - wenn **Komponenten** verwendet werden, die **nicht mit den existierenden Bausteinen** des IT-Grundschutz-Kompodiums **abgebildet** werden können

ist zu prüfen, ob sich zusätzliche Sicherheitsanforderungen ergeben und damit zusätzliche oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind (**Risikoanalyse**)



Nachweis der Umsetzung von IT-Grundschutz

- Der **Nachweis** über die erfolgreiche Umsetzung von IT-Grundschutz durch einen **unabhängigen** BSI zertifizierten IT-Grundschutz Auditor kann die Bemühungen für die Informationssicherheit nach Innen oder Außen sichtbar zu machen (Kunden, Partner, Öffentlichkeit)
- Die Basis-Absicherung kann mit dem **Testat nach der Basis-Absicherung** nachgewiesen werden
- Die Standard- bzw. Kern-Absicherung kann mit der **ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz** nachgewiesen werden



Warum ein ISMS für einen Notfall nicht immer ausreicht

Artikel 1: „Et es wie et es.“

Sieh den Tatsachen ins Auge, du kannst eh nichts ändern.

Artikel 2: „Et kütt wie et kütt.“

Füge dich in das Unabwendbare; du kannst ohnehin nichts am Lauf der Dinge ändern.

Artikel 3: „Et hätt noch emmer joot jejange.“

*Was gestern gut gegangen ist, wird auch morgen funktionieren.
Situationsabhängig auch: Wir wissen es ist „Murks“, aber es wird schon gut gehen.*

...

Artikel 7: „Wat wells de maache?“

Füg dich in dein Schicksal.

...

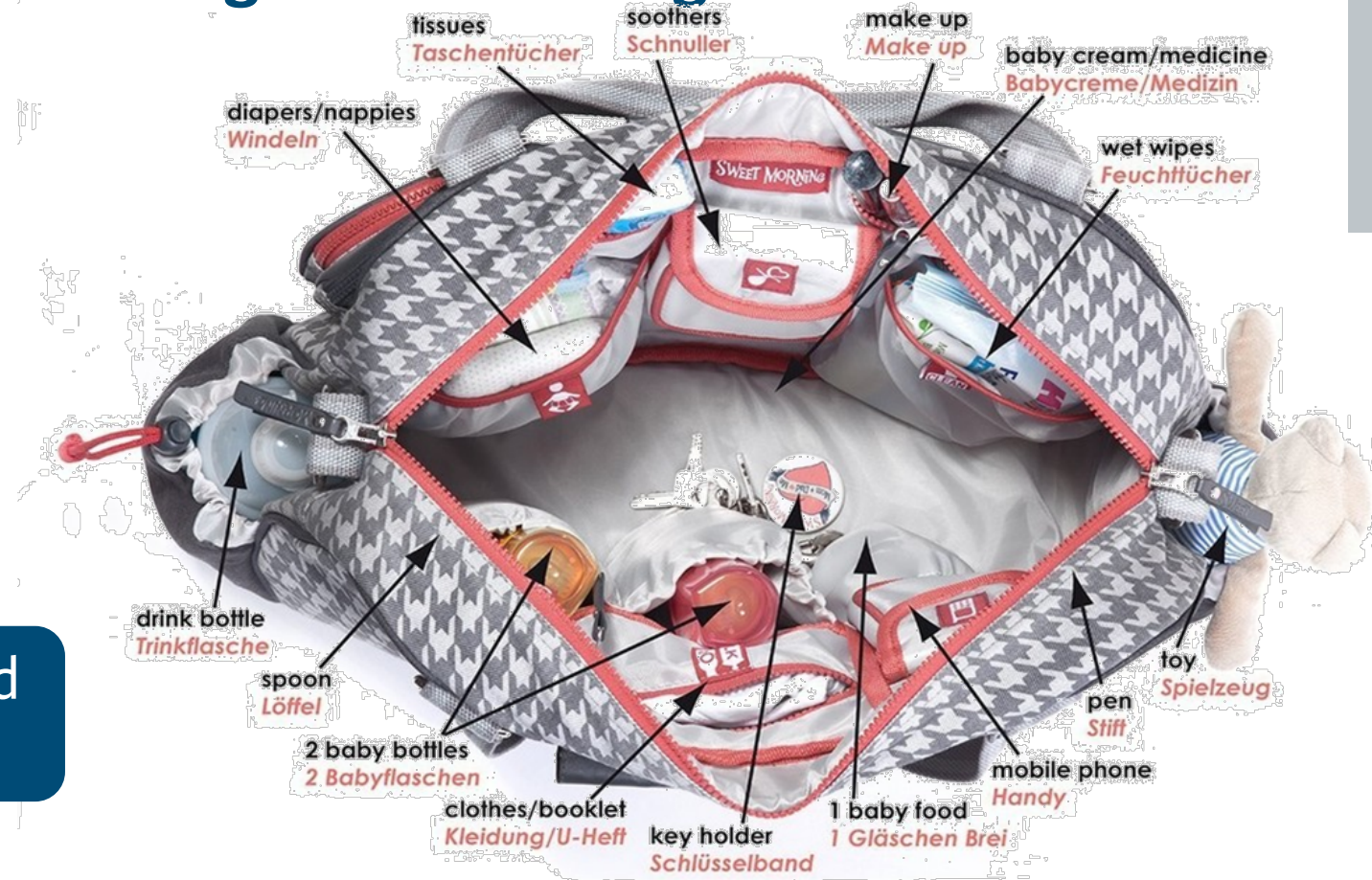
Warum ein ISMS für einen Notfall nicht immer ausreicht

Notfallmanagement im Alltag – eine Analogie

Notfallmanagement, d.h. Vorbereitung und Vermeidung von Notfällen erfolgt im Alltag häufig unbewusst und „von selbst“.



In Institutionen viel komplexer und kaum „nebenbei“ zu erledigen



Warum ein ISMS für einen Notfall nicht immer ausreicht

Ein weiteres Beispiel aus der Praxis

Übersicht über die Ereignisse

- Nicht-gezielter Angriff
 - Computervirus konnte nicht eingedämmt werden
- Die gesamte IT wurde abgeschaltet (weil es einen **Notfallplan** dafür gab)
- Notbetrieb unter verschärften Bedingungen

Nur durch ein präventives Notfallmanagement war ein weiterer Betrieb im Notfall möglich



11. Februar 2016 | 13.04 Uhr

Hacker-Angriff in Neuss

Computer-Virus legt das Lukaskrankenhaus lahm



Ärzte und Patienten wurden über den System-Ausfall mittels Flugblättern informiert.

FOTO: Andreas Woitschütze

www.atex.com

Von Sebastian Bergmann

Deutschland
Digital•Sicher•BSI

IT-Grundschutz

Deutschland
Digital•Sicher•BSI•

Vielen Dank für Ihre Aufmerksamkeit!

Christoph Wiemers

grundschutz@bsi.bund.de
Tel. +49 (0)22899-9582-5369

Bundesamt für Sicherheit in der Informationstechnik
Referat „BSI-Standards und IT-Grundschutz“
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik