IT-Sicherheit erhöhen
Tipps aus der Praxis

10.04.2019

Was nun?

IT-Sicherheit

IT-Sicherheit = Informationssicherheit

IT-Sicherheit

Vertraulichkeit

Daten vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen

Verfügbarkeit

IT-Services (Hardware, Software, Funktionen) stehen zur richtigen Zeit am richtigen Ort zur Verfügung

Integrität

Vollständigkeit und Korrektheit von Daten

IT-Sicherheit

Ziel

Risiken, durch angemessenen Massnahmen, **auf ein akzeptables Mass reduzieren**

Orientierungshilfen

- Diverse Merkblätter, Checklisten und Standards
  - Merkblatt Informationssicherheit für KMUs, MELANI
  - Cybersecurity-Schnelltest für KMU, ICT SWITZERLAND
    https://ictswitzerland.ch/themen/cyber-security/check/
  - ISO 27000-Reihe
  - Etc.

- IT-Grundschutz-Kompendium 2019

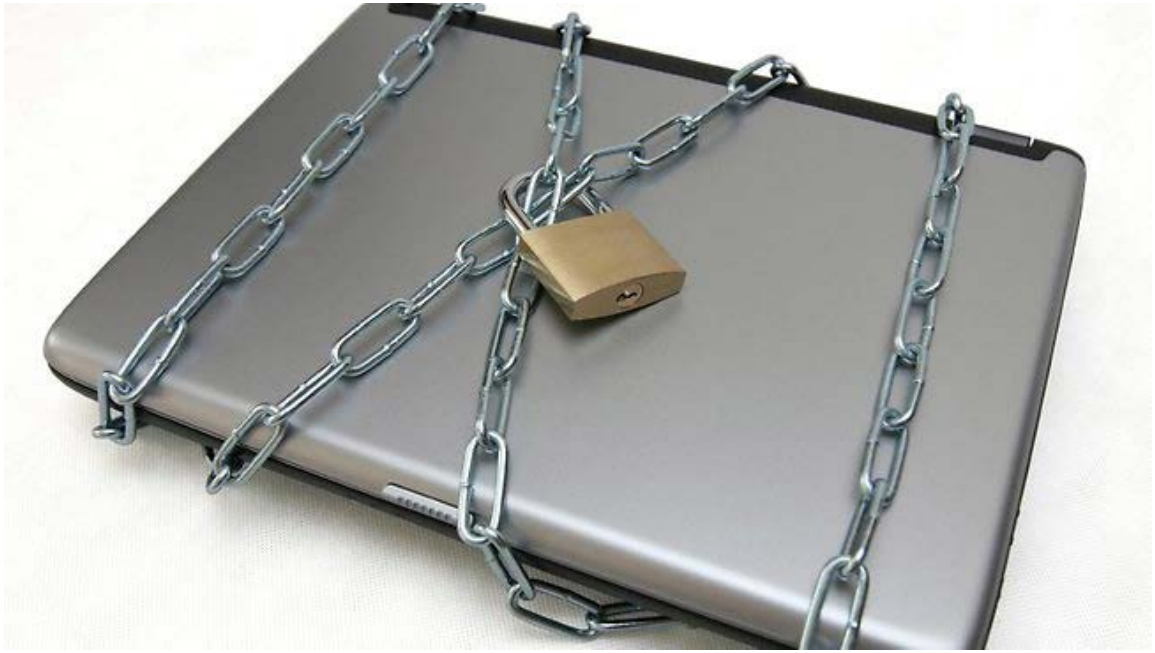
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_no

  - Konkrete Empfehlungen und Anleitungen
  - 10 Schichten / 94 Bausteine
  - Priorisierung

Bundesamt
für Sicherheit in der
Informationstechnik

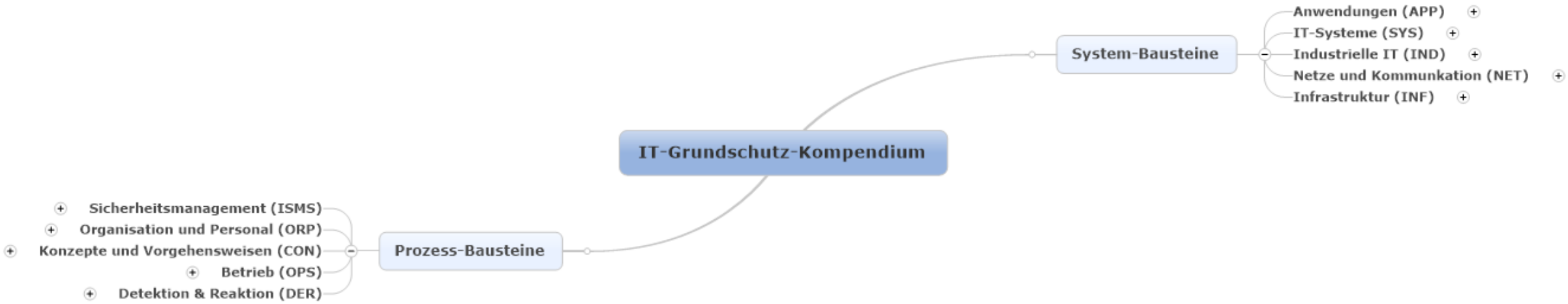
Zwei Dimensionen

System / Technisch

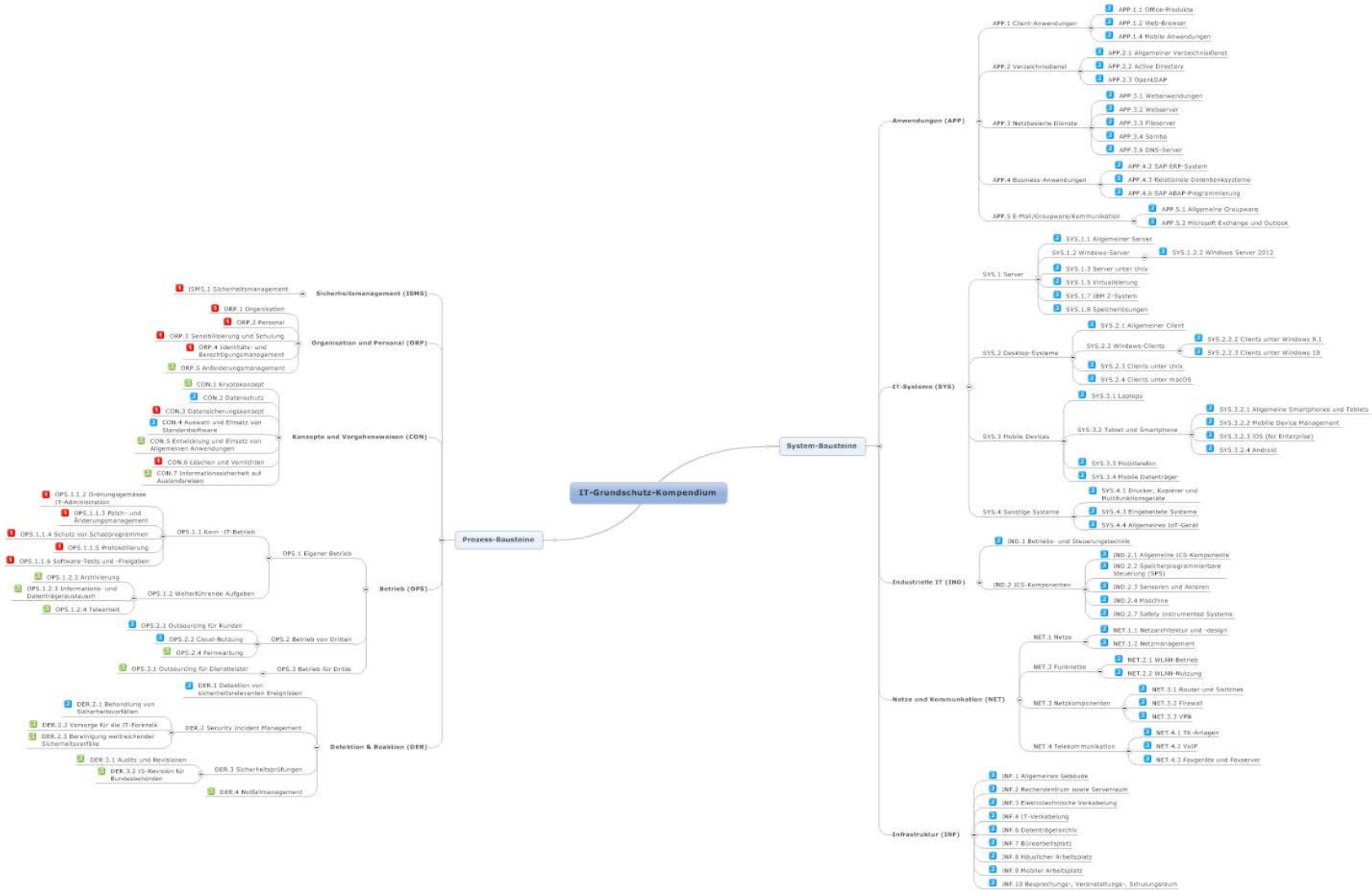


Organisatorisch / Prozessual

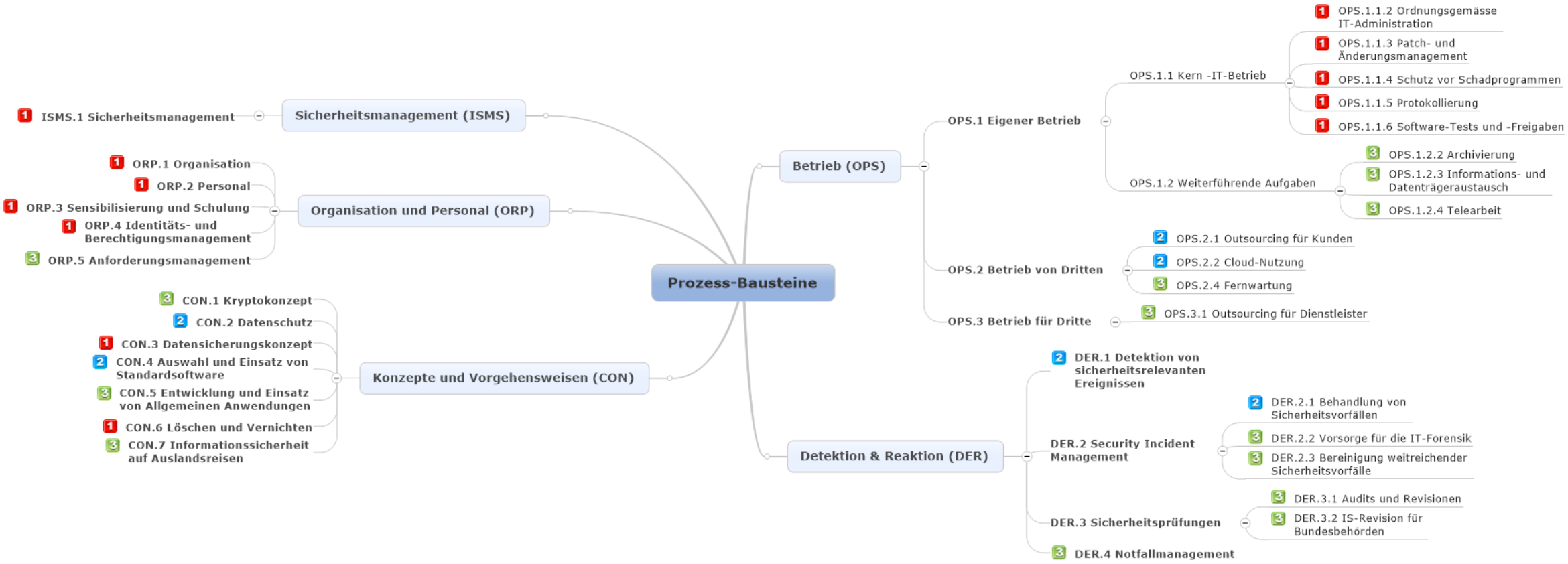
IT-Grundschutz-Kompendium 2019



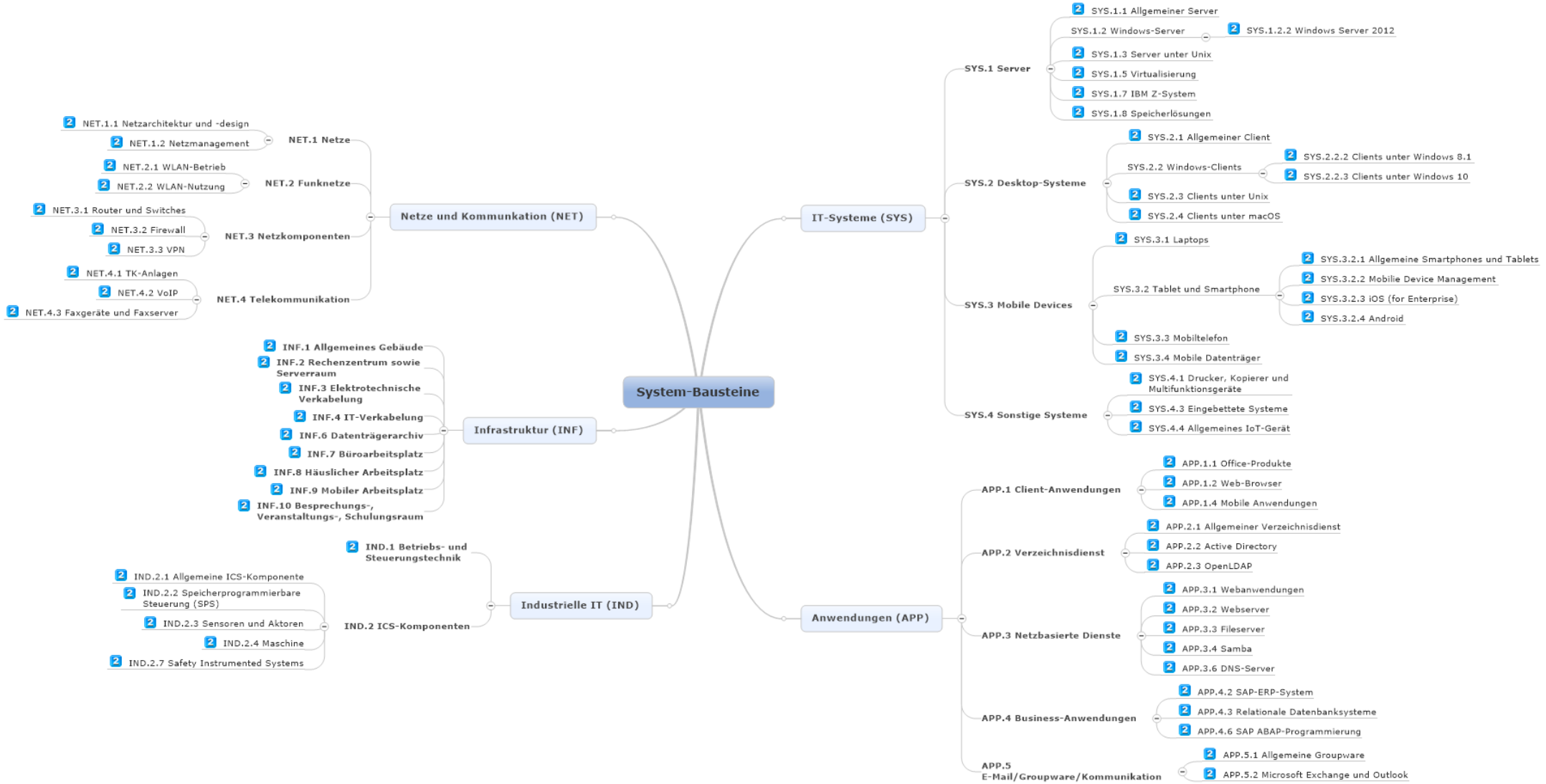
IT-Grundschutz-Kompendium 2019



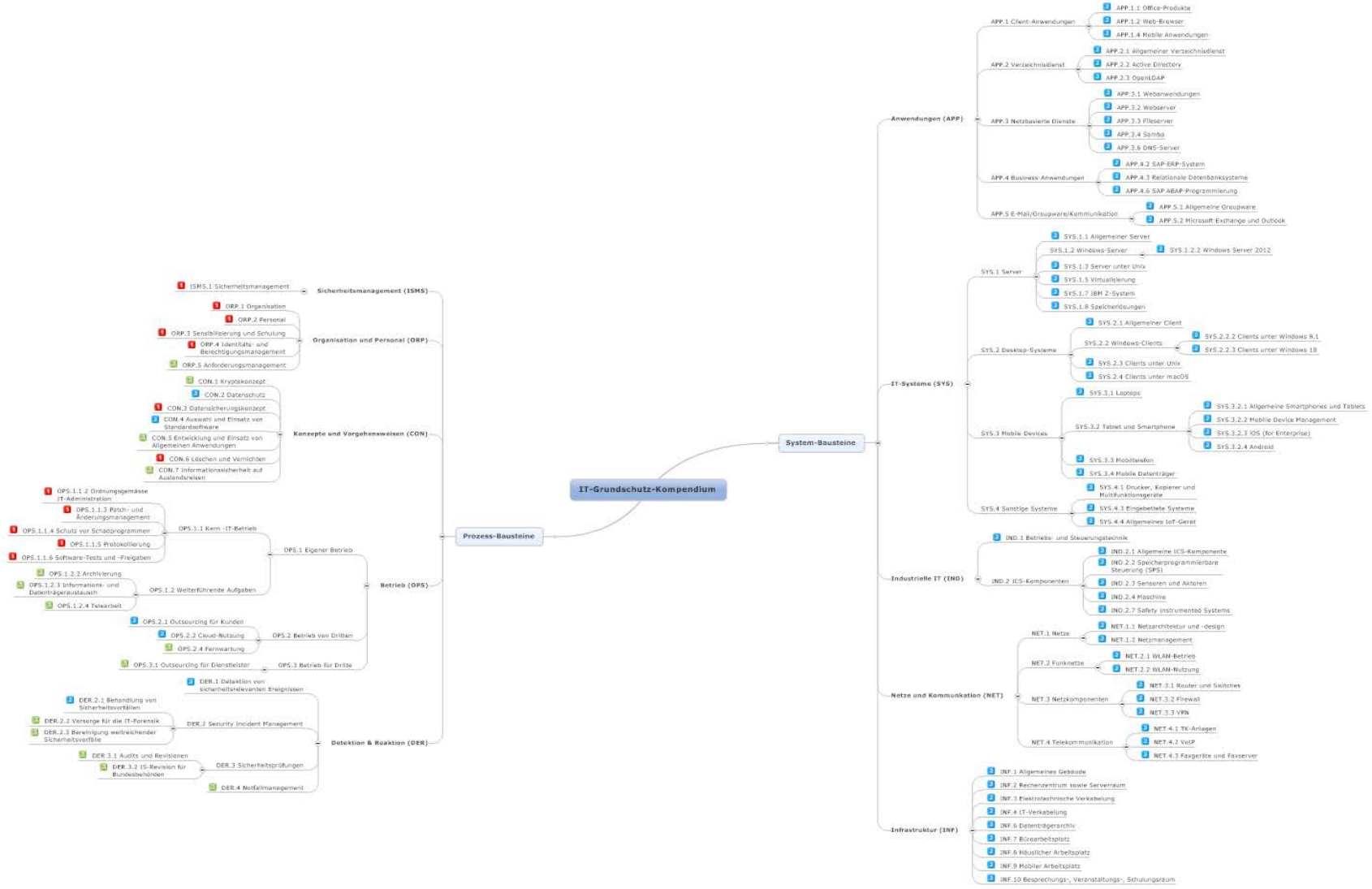
IT-Grundschutz-Kompendium 2019



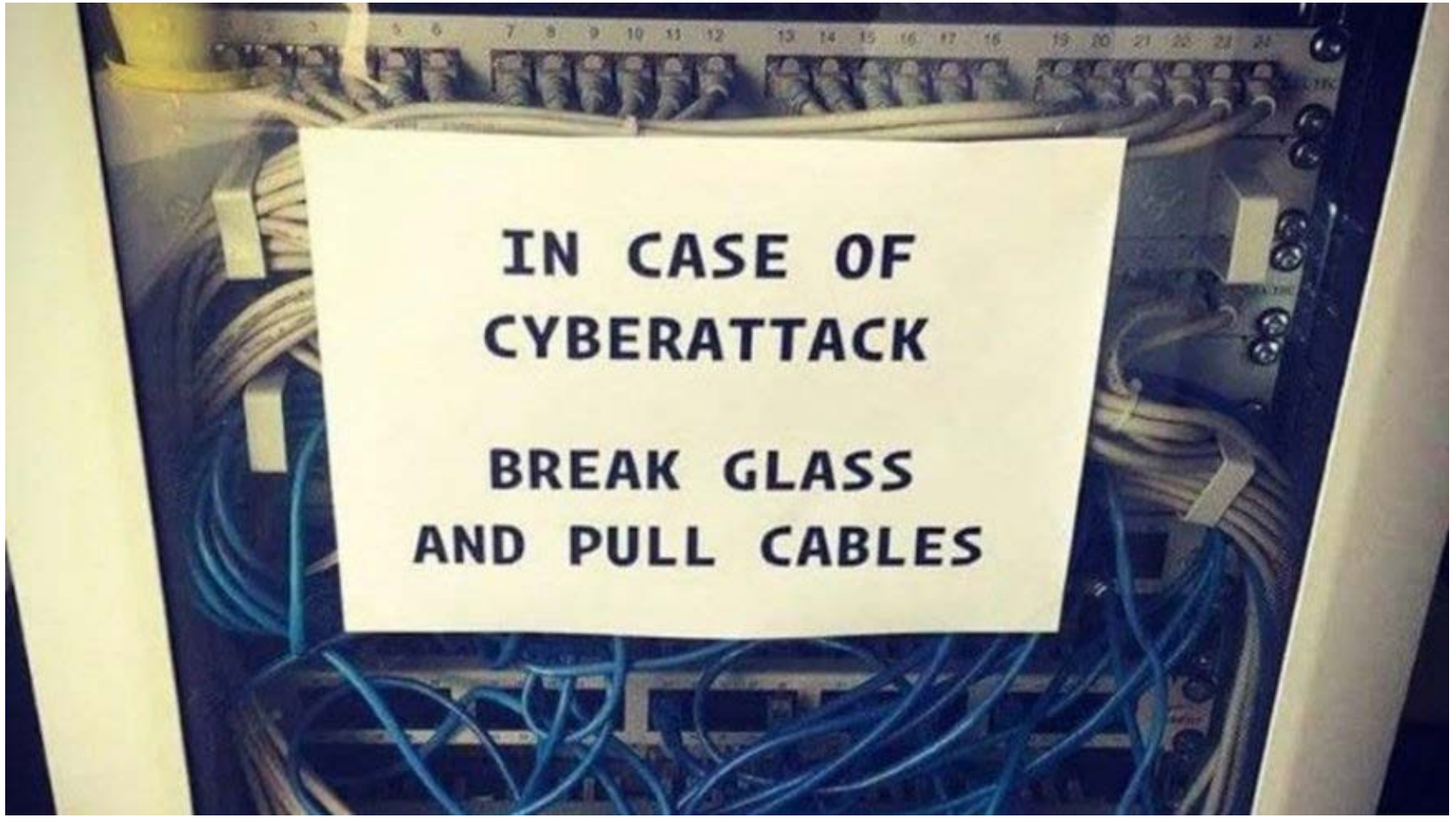
IT-Grundschutz-Kompendium 2019



IT-Grundschutz-Kompendium 2019



Tipps aus der Praxis



Tipps aus der Praxis (1/4)

- IT-Strategie
  - Abgeleitet aus der Geschäftsstrategie
- IT-Governance
  - Definition Führung, Organisationsstruktur und Prozesse zur Sicherstellung, dass die IT die Unternehmensstrategie unterstützt
  - Entscheidungsmatrix, Auftrag an die IT, Richtlinien, Regeln, Vorgaben
- IT-Prozesse
  - Gelebt
- Leitlinie IT-Sicherheit
  - Relevante Gesetze, Normen, Vorschriften
  - Büroräume, Arbeitsplätze, Verhalten Personal, etc.
  - Maximale Systemausfallzeiten definieren
  - Maximalen akzeptablen Datenverlust definieren
  - Notfallkonzepte (z.B. bei IT-Ausfall, Datenverlust, etc.)
  - In IT-Projekten berücksichtigen
- Datenverarbeitungsinventar

Tipps aus der Praxis (2/4)

- Evaluation neuer Hard- und Software
  - Strukturiertes, methodisches Vorgehen
  - Gewährleisten einer homogenen, integralen Systemlandschaft
  - Rechtliche Verpflichtung
    - Ausschreibung / Submission
- Externe Audits periodisch durchführen lassen
  - Umfassende IT-Sicherheitsaudits, nicht nur IKS-Vorgaben
  - Wechselnde Auditoren
- Schulungen für Mitarbeitende
  - Regelmässig Sensibilisierung für IT-Sicherheit
  - Allgemeine Schulungen
- Zugriffskonzepte für die wichtigen Systeme und Softwares
  - Einhaltung regelmässig überprüfen

Tipps aus der Praxis (3/4)

- Backup
  - Regelmässig prüfen, ob erfolgreich
  - Wiederherstellungstests
- Erlaubte Dateiendungen
  - Einschränken auf Fileserver
    - Ransomware
- Automatismen zur Erkennung von verdächtigen Vorgängen
  - Einrichten auf Fileserver
    - z.B. 50 Speichervorgänge pro Minute → Automatisches Sperren des Benutzers
- E-Mails
  - Verschlüsselung
  - E-Mails auf mobile Geräte synchronisieren
    - Mobile Device Management
    - Zusätzliche Schutzmassnahmen, welche auf den Geräten erzwungen werden können (z.B. PIN-Code)
- Website
  - Keine direkten Kontaktdaten von Mitarbeitenden aufführen
    - Spear Phishing (z.B. E-Mail Adresse Geschäftsführer)

Tipps aus der Praxis (4/4)

- Lieferanten / IT-Partner
  - Detaillierte Verträge
    - Zu erbringenden Leistungen eindeutig festgehalten
    - Regelmässig prüfen und nötigenfalls überarbeiten
    - Einhaltung der eigenen Vorgaben zur Informationssicherheit
    - Beinhaltet auch Einhaltung der Datenschutzgesetze
  - Leistungserbringung unabhängig von Einzelpersonen
- Jährlich wiederkehrende Budgetposition für IT-Sicherheit
  - Geben Sie das Geld aus!

Fragen?

Vielen Dank für Ihre Aufmerksamkeit

tobias.fessler@itmb.ch | 079 590 23 40