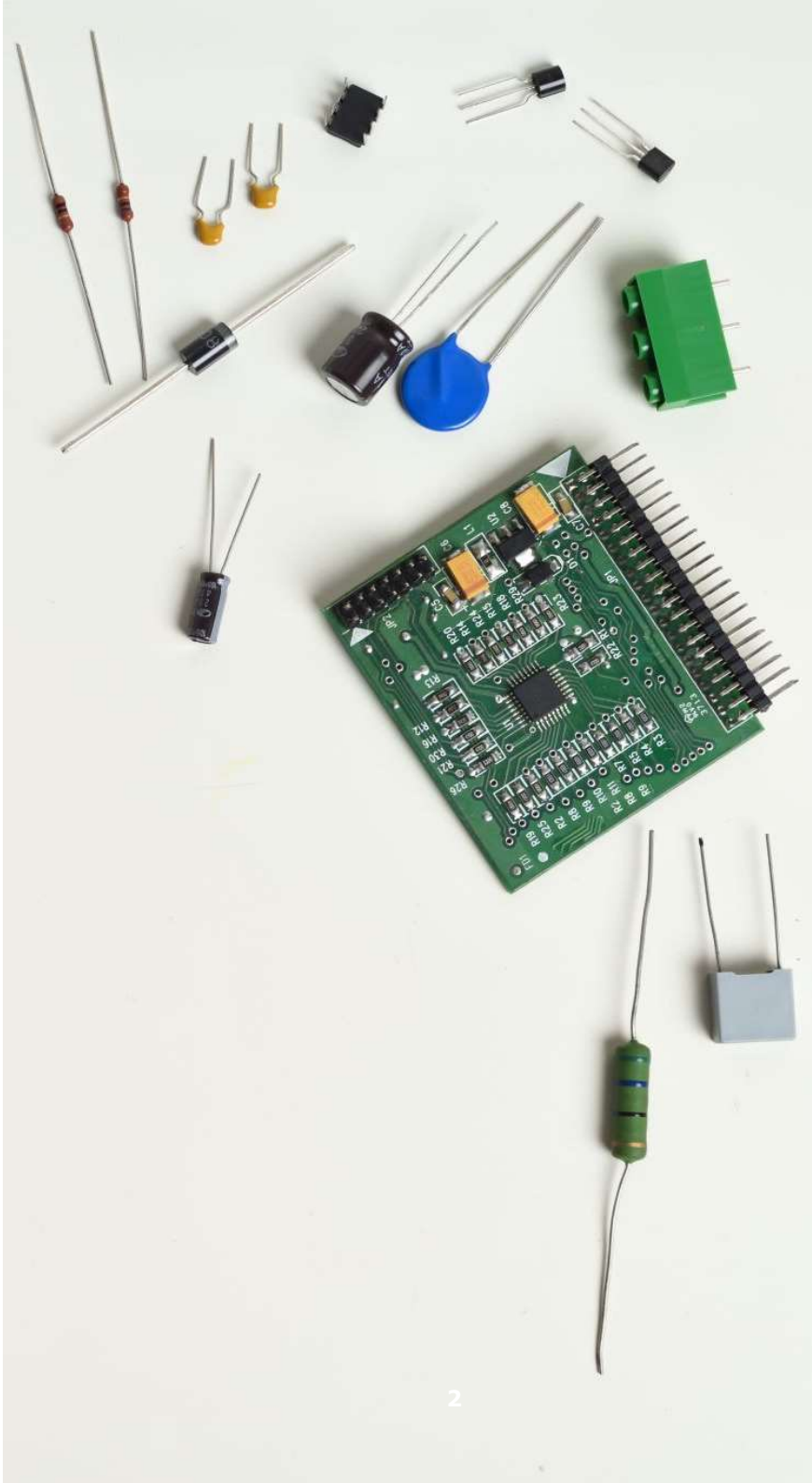
Risikofaktor Mensch in der IT-Security

Wilfried Andexer

- ✓ IT-Berater
- ✓ ASAP Digital Solutions GmbH
- ✓ ISO 27001 Auditor und Berater
- ✓ NIS-Prüfer



Risikofaktor Mensch

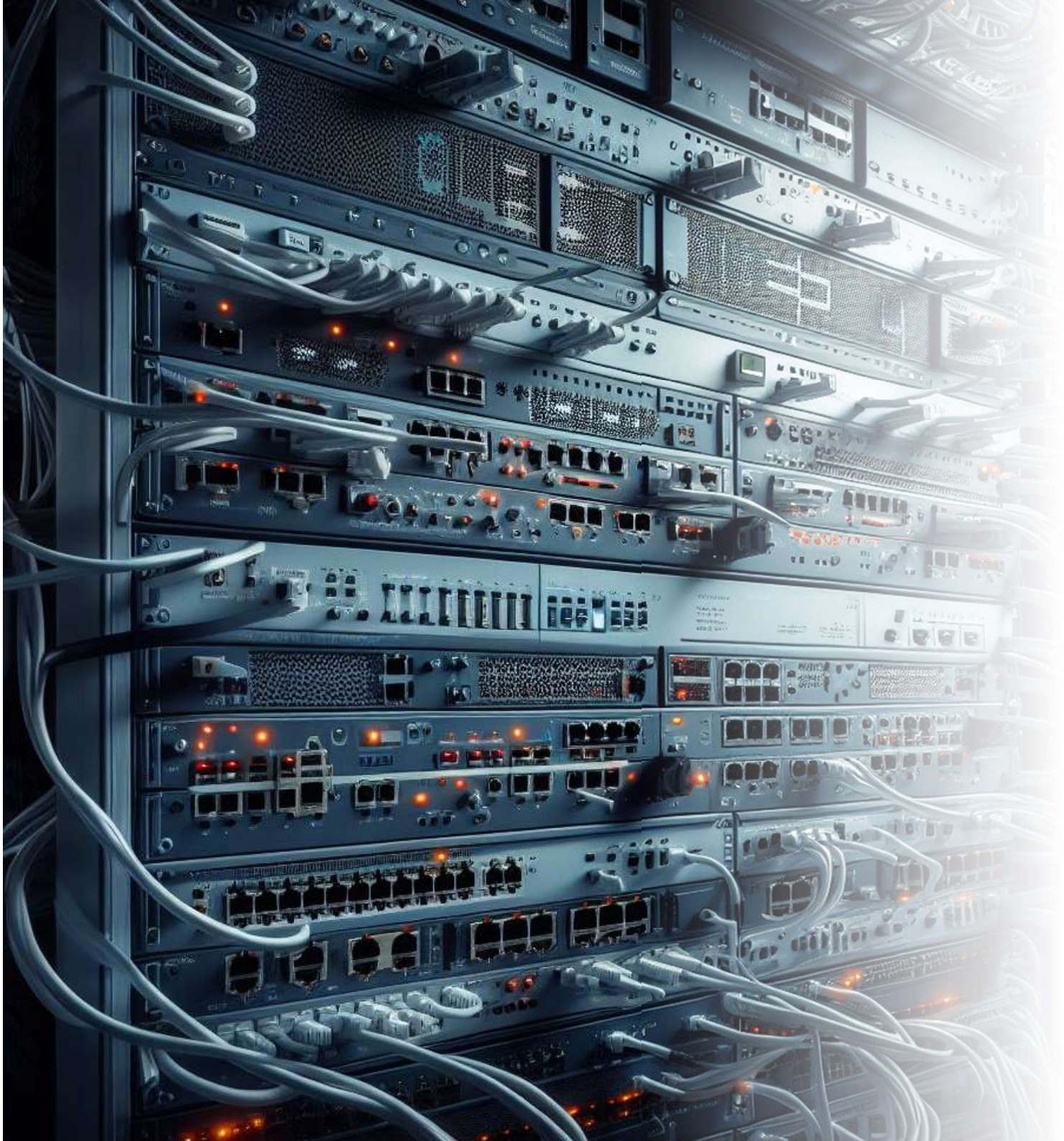
Wie können wir unser Unternehmen schützen?

Physische Maßnahmen

- Mauern
- Zäune
- Türen
- Alarmanlagen
- Schlüssel
- Fenster

Organisatorische Maßnahmen

- Passwort-Regeln
- Verhaltensregeln
- Prozessbeschreibungen
- Notfallhandbuch
- Up-to-date bleiben
- ...



Technische Maßnahmen

- Firewalls
- VLANs
- VPNS
- Backups
- Zugangskontrolle
- ...

Menschliche Maßnahmen

- Schulung
- Geheimhaltung
- Verträge
- Neueinstellung
- Beendigung Dienstverhältnis

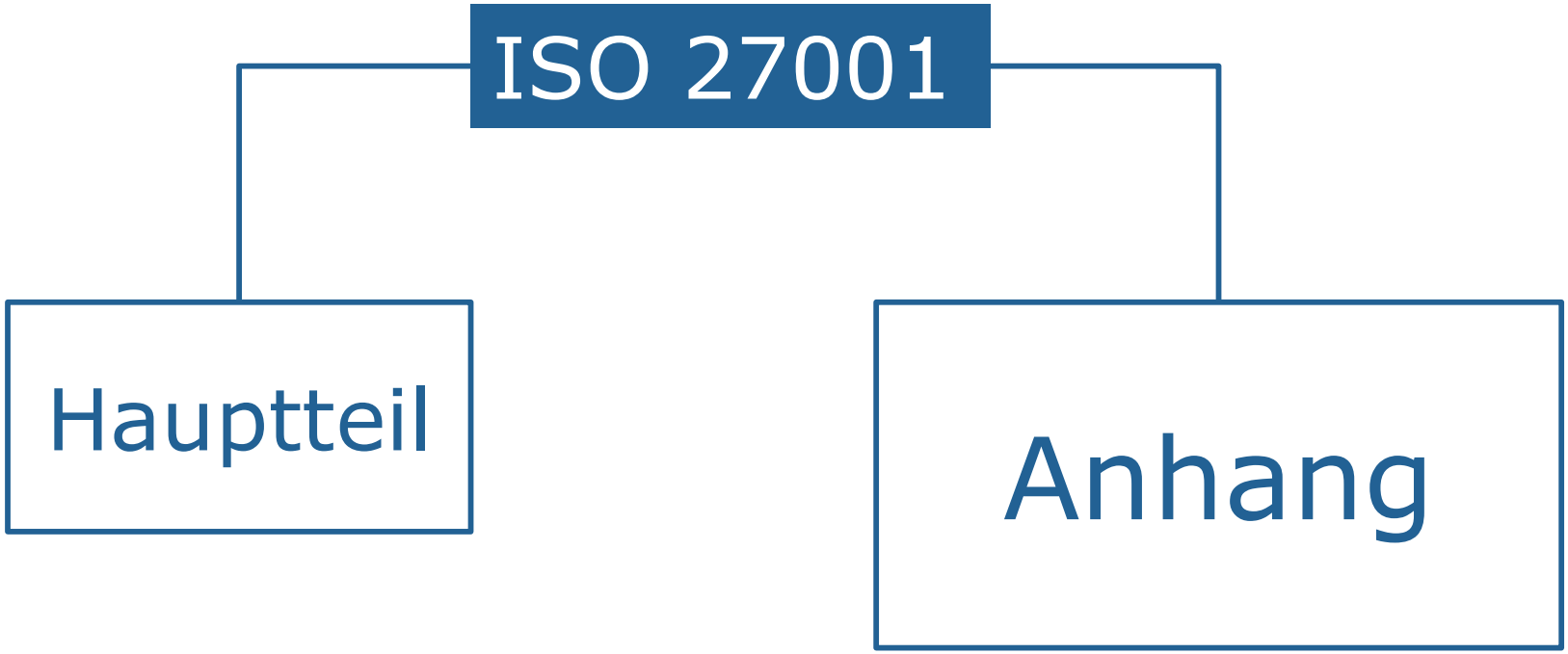
Dafür gibt es ein Framework...

ISO 27001

Internationaler Standard für die Informationssicherheit

- „spezifiziert die Anforderungen für ... ein **Informationssicherheitsmanagementsystem** (ISMS)..."
- **Ganzheitlicher Ansatz**
  - **Nicht nur technische Maßnahmen**
- **Kontinuierliche Verbesserung**
- **Risikobasierter Ansatz**
  - **Was ist bedroht?**
  - **Wie wird geschützt?**

ISO 27001



ISO 27001 Hauptteil

Kontext

Planung

Betrieb

Verbesserung

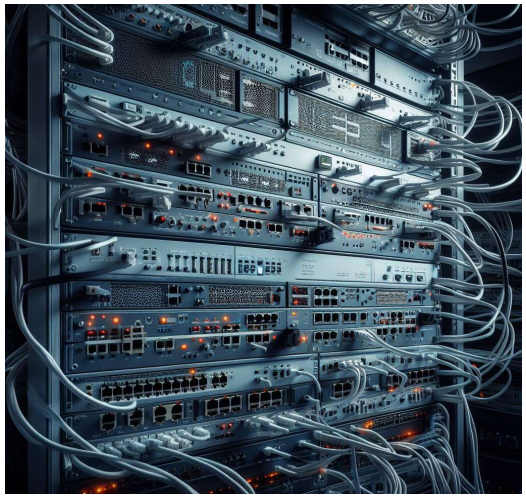
...

ISO 27001 Anhang Maßnahmen

A.5 organizational

A.6 People

A.7 physical



A.8 technological

Reine Theorie! Und in der Praxis?

Beispiel 1: Solarwinds

- **SolarWinds was the subject of a massive cybersecurity attack that spread to the company's clients.**
- **Major firms like Microsoft and top government agencies were attacked, and sensitive data was exposed.**

businessInsider

IT-SECURITY

Solarwinds: Passwort für gehackten Update-Server lautete "solarwinds123"

DerStandard

ISO 27001 Maßnahme

A.8.1 Privileged access rights

Beispiel 2: Donald Trump

Trump's Twitter account was hacked, Dutch ministry confirms

TheGuardian

NETZPOLITIK 23

"maga2020!" als Passwort: Niederländische Staatanwaltschaft bestätigt Trumps Twitter-Hack

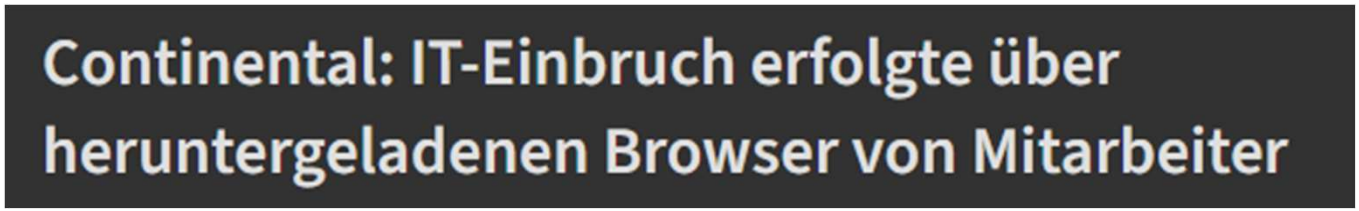
DerStandard

ISO 27001 Maßnahme

8.5 Secure authentication

Beispiel 3: Continental

Ndr.de



heise.de

ISO 27001 Maßnahme

A.8.19 Installation of software on operational systems

Beispiel 4: EZB

EZB: Cyberangriff auf Präsidentin Lagarde – keine Daten geklaut

Handelsblatt.com

Einem Bericht des Portals „Business Insider“ vom Dienstag zufolge, wurde Lagarde mit der scheinbar echten Handynummer der ehemaligen Bundeskanzlerin Angela Merkel (CDU) kontaktiert.

Handelsblatt.com

ISO 27001 Maßnahme

A.6.3 Information security awareness, education and training

Vielen Dank für die Aufmerksamkeit!

Speziellen Dank an:

Image Creator
powered by **DALL·E 3**

ASAP Digital Solutions GmbH
Ginzkeyplatz 10/2
A-5020 Salzburg
www.asapdigital.com
Tel.: +43 662 24 30 22