IT Grundschutzcheck

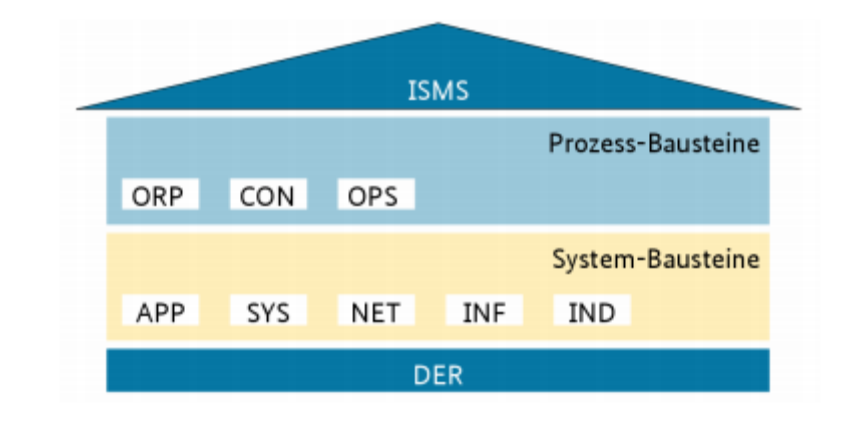
NACH VORGABE DES BSI
(BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNOLOGIE)

Themen

- **Was ist der BSI Grundschutz ?**
- Wahl der Vorgehensweise
- Vorgehensweise
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - Schutzbedarfsbestimmung
  - Modellierung
  - Grundschutzcheck (Soll / Ist Analyse)
  - Handlungsempfehlungen

Was ist BSI Grundschutz

- Basiert auf der Norm ISO 27001
- Erweitert um das Grundschutzkompendium
  - Konkrete Handlungsvorschläge durch sogenannte Bausteine



Beispiel:
Baustein App 1.2 (Webbrowser)

APP.1.2.A2 Verschlüsselung der Kommunikation

Der Web-Browser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Unsichere Versionen von TLS SOLLTEN deaktiviert werden. Der Web-Browser MUSS den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen. Für alle wichtigen öffentlichen TLS-verschlüsselten Web-Dienste SOLLTEN die Domains in die HSTS-Preload-Liste des Browsers eingefügt werden.

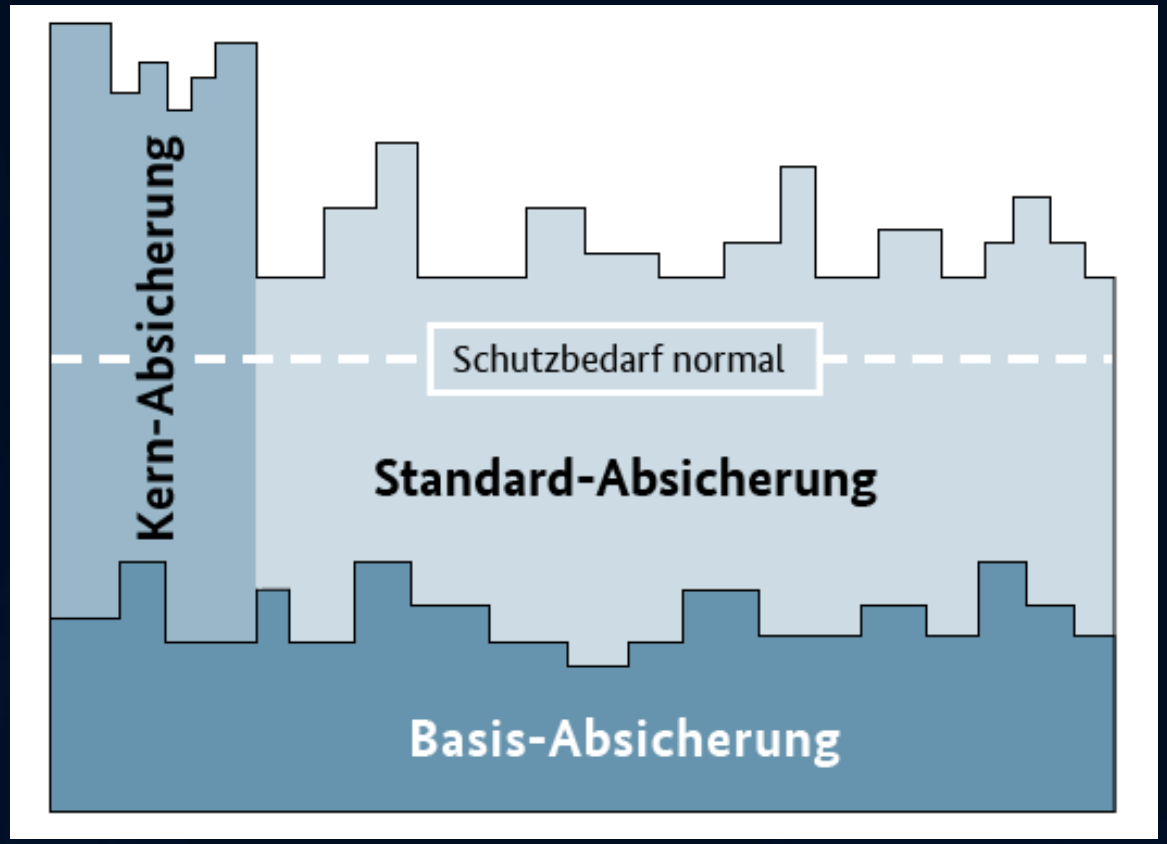
Themen

- Was ist der BSI Grundschutz ?
- **Wahl der Vorgehensweise**
- Vorgehensweise
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - Schutzbedarfsbestimmung
  - Modellierung
  - Grundschutzcheck (Soll / Ist Analyse)
  - Handlungsempfehlungen

Wahl der Vorgehensweise

- Basisabsicherung
  - Guter Grundstandard als Einstieg
  - Nicht Zertifizierungsfähig nach ISO 27001
- Kernabsicherung
  - Betrachtet nur die “kritischen” Unternehmensteile
  - Zertifizierungsfähig nach ISO 27001
- Standardabsicherung
  - Das erklärte Ziel des BSI
  - Zertifizierzungsfähig nach ISO 27001

Wahl der Vorgehensweise



Themen

- Was ist der BSI Grundschutz ?
- Wahl der Vorgehensweise
- **Vorgehensweise**
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - Schutzbedarfsbestimmung
  - Modellierung
  - Grundschutzcheck (Soll / Ist Analyse)
  - Handlungsempfehlungen

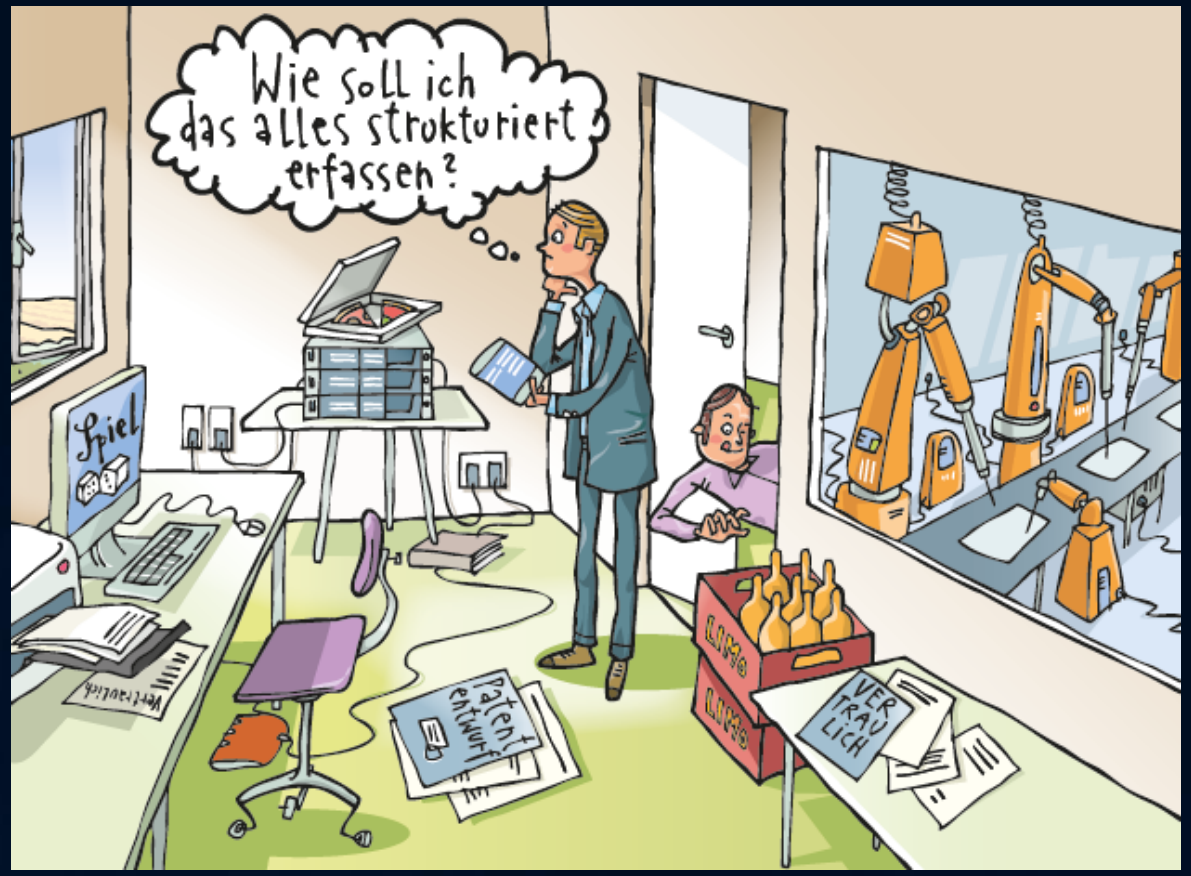
Themen

- Was ist der BSI Grundschutz ?
- Wahl der Vorgehensweise
- Vorgehensweise
  - **Festlegen der Zielobjekte durch die Strukturanalyse**
  - Schutzbedarfsbestimmung
  - Modellierung
  - Grundschutzcheck (Soll / Ist Analyse)
  - Handlungsempfehlungen

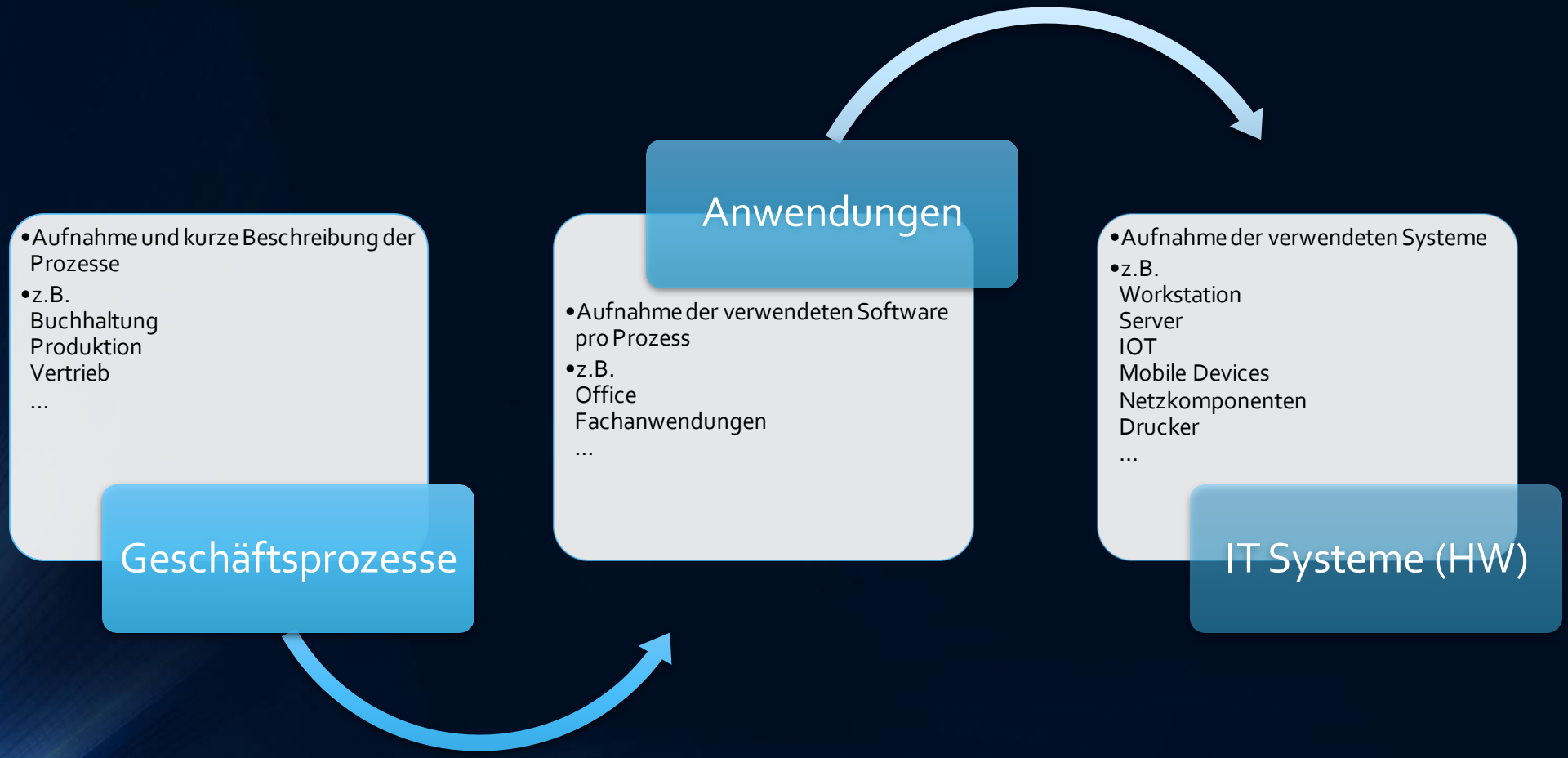
Zielobjekte

- Software
- Hardware
- Netzwerkkomponenten
- Telekommunikationseinrichrungen
- Räume
- Prozesse

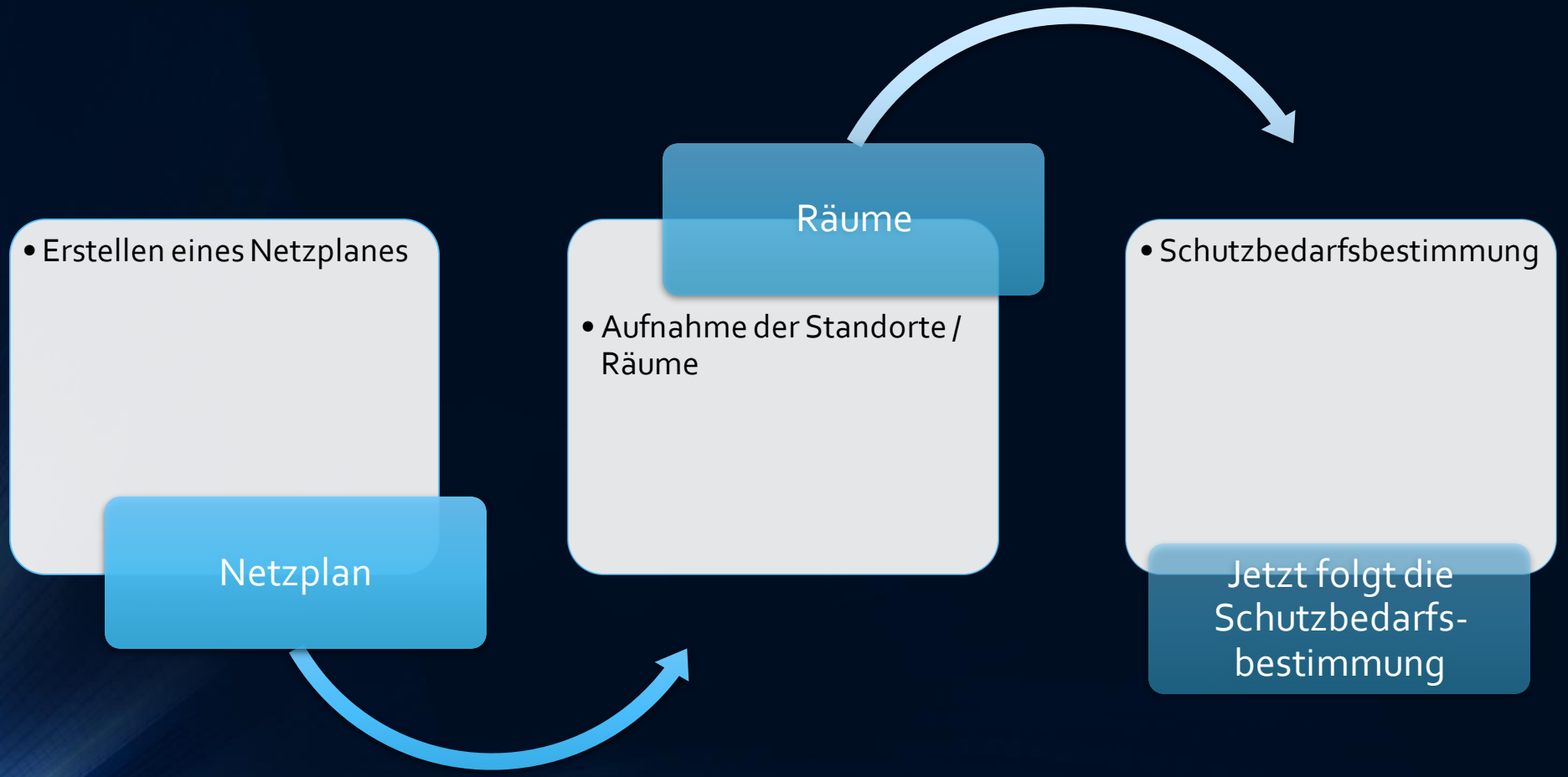
Strukturanalyse



Strukturanalyse - 1



Strukturanalyse - 2



Themen

- Was ist der BSI Grundschutz ?
- Wahl der Vorgehensweise
- Vorgehensweise
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - **Schutzbedarfsbestimmung**
  - Modellierung
  - Grundschutzcheck (Soll / Ist Analyse)
  - Handlungsempfehlungen

Schützenswerte Grundwerte

- Verfügbarkeit
- Vertraulichkeit
- Integrität

Schadenskategorien

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
- Beeinträchtigungen der persönlichen Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung oder
- finanzielle Auswirkungen.

Schutzbedarfskategorien

- Normal
- Hoch
- Sehr hoch

Beispiel für Schadenskategorie Finanzielle Auswirkungen und Erfüllung der Aufgaben. Fragestellung: Was wäre wenn ….

	Verfügbarkeit	Vertraulichkeit	Integrität
Normal	Eine Nichtverfügbarkeit von mehr als 24 Stunden ist tolerabel. Der finanzielle Schaden ist akzeptabel	Ein Verlust der Vetraulichkeit ist führt zu keinen gravierenden Schäden.	Ein Verlust der Integrität führt zu keinem gravierenden finanziellen Schaden und hat keine Auswirkung auf die Aufgabenerfüllung
Hoch	Eine Nichtverfügbarkeit von mehr als 12 Stunden ist nicht tolerabel. Der finanzielle Schaden ist beträchtlich	Ein Verlust der Vetraulichkeit führt zu massiven Verstößen gegen geltendes Recht. Es ist mit hohen Bußgeldern zu Rechnen.	Ein Verlust der Integrität führt zu massiven Schäden durch stehende Produktion.
Sehr hoch	Eine Nichtverfügbarkeit von mehr als 1 Stunde ist nicht vertretbar. Der Finanzielle Schaden ist existenzbedrohend.	Ein Verlust der Vetraulichkeit führt zu massiven Verstößen gegen geltendes Recht. Es ist mit sehr hohen Bußgeldern und Sanktionen zur rechnen, die existenzbedrohend sein können	Ein Verlust der Integrität führt zu existenzbedrohenden Schäden durch stehende Produktion

Anwendung auf ein Zielobjekt.
Bsp: Lagerwaltungssystem

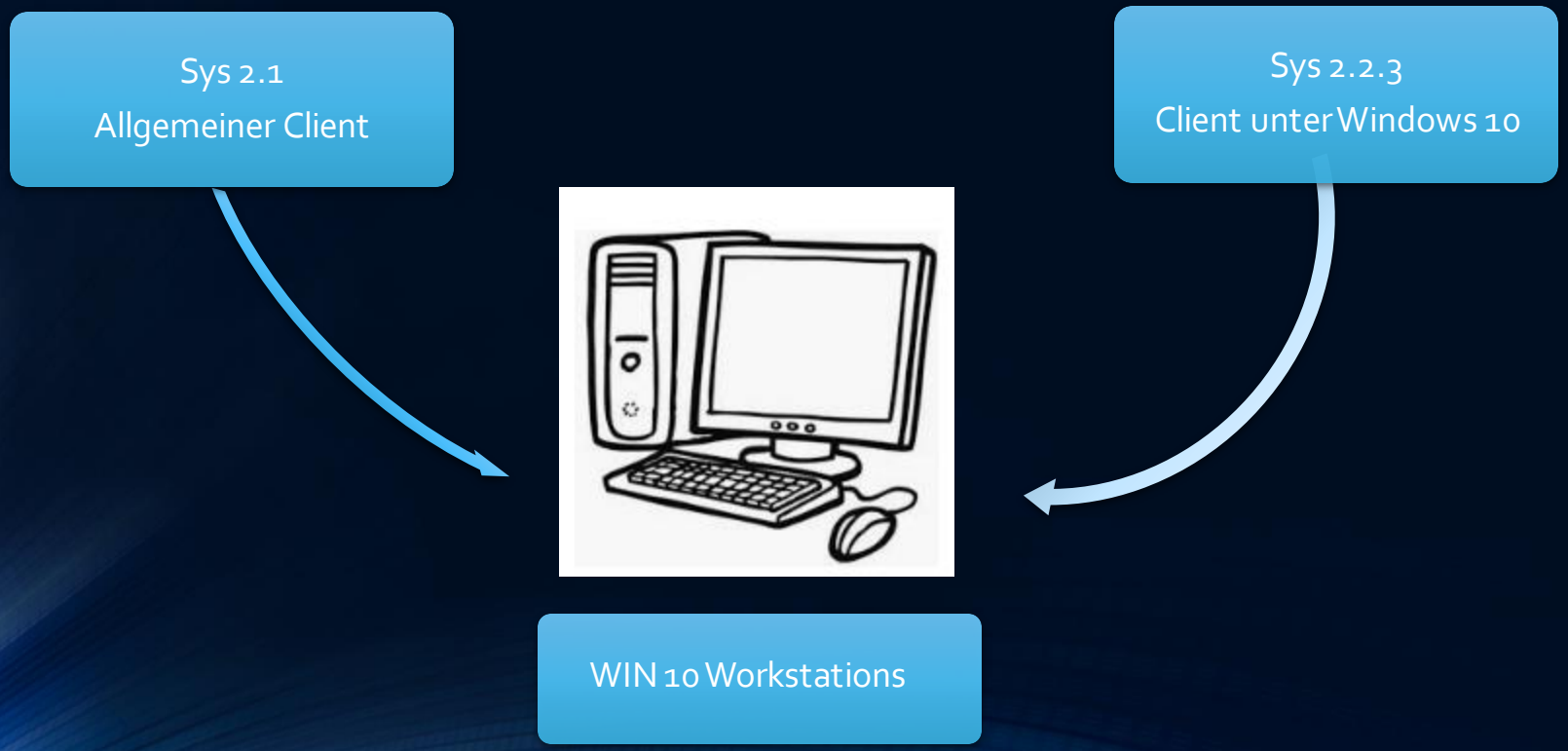
	Kategorie	Begründung
Vertraulichkeit	Normal	Die in dem System verwalteten Daten (Artikel Standorte der Artikel im Lager) sind für unberechtigte Dritte nicht von Nutzen.
Verfügbarkeit	Hoch	Bei einem Ausfall des Systems ist das Unternehmen nicht mehr Lieferbereit. Es sind hohe Konventionalstrafen wegen Lieferverzug zu erwarten.
Integrität	Hoch	Ein Integritätsverlust würde den Verlust der Kontrolle über den Lagerbestand bedeuten. Dies würde die Lieferfähigkeit beinträchtigen, und könnte zu Konventionalstrafen führen.

Themen

- Was ist der BSI Grundschutz ?
- Wahl der Vorgehensweise
- Vorgehensweise
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - Schutzbedarfsbestimmung
  - **Modellierung**
  - Grundschutzcheck (Soll / Ist Analyse)
  - Handlungsempfehlungen

Modellierung

- Anwendung der Bausteine des Grundschutzkomendiums auf die Zielobjekte, hier am Beispiel eines Windows 10 Clients.

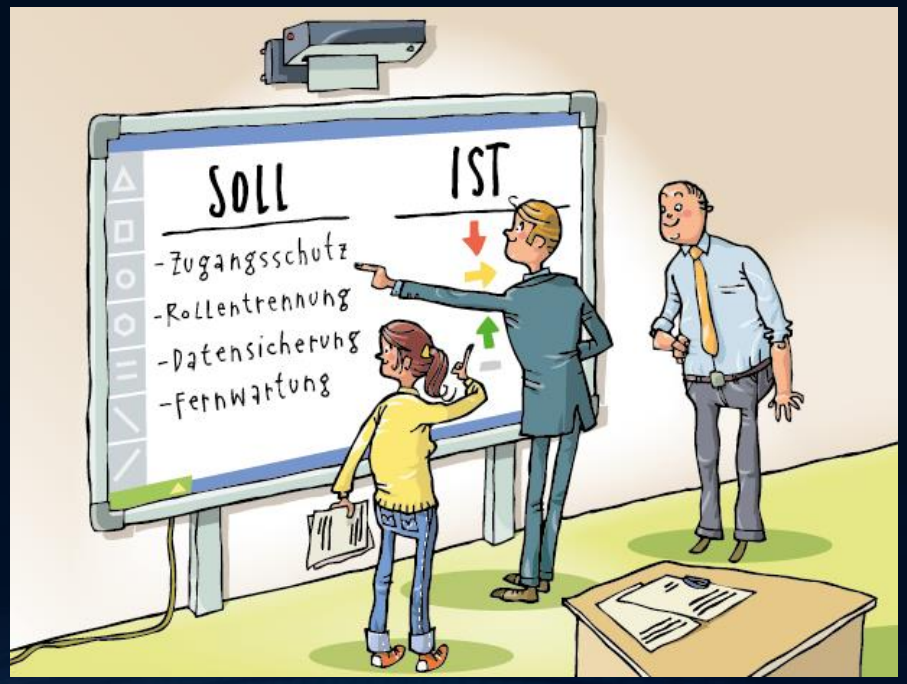


Themen

- Was ist der BSI Grundschutz ?
- Wahl der Vorgehensweise
- Vorgehensweise
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - Schutzbedarfsbestimmung
  - Modellierung
  - **Grundschutzcheck (Soll / Ist Analyse)**
  - Handlungsempfehlungen

Grundschutzcheck

- Soll – Ist Vergleich der Anforderungen der modellieren Bausteine gegen den IST - Zustand
- Gegebenenfalls folgt eine Risikoanalyse



Themen

- Was ist der BSI Grundschutz ?
- Wahl der Vorgehensweise
- Vorgehensweise
  - Festlegen der Zielobjekte durch die Strukturanalyse
  - Schutzbedarfsbestimmung
  - Modellierung
  - Grundschutzcheck (Soll / Ist Analyse)
  - **Handlungsempfehlungen**

Handlungsempfehlungen / Umsetzungsplan

Anforderung: **Umzusetzende Maßnahme**	**Termin**	**Budget**	**Umsetzung durch**
SYS.1.1.A3 *Restriktive Rechtevergabe:* Die verbliebenen Gruppenberechtigungen müssen aufgelöst werden.	Drittes Quartal des Jahres	keine Kosten	Herr Schmitt (IT-Betrieb)
SYS.1.1.A4 *Rollentrennung*: Separate Benutzerkennungen für jeden Administrator einrichten	31. Juli des Jahres	keine Kosten	Herr Schmitt (IT-Betrieb)
SYS.1.1.A8 *Regelmäßige Datensicherung:* Die Datensicherungen werden derzeit auf Bändern im Serverraum aufbewahrt. Ein externes Backup-System ist geplant. Ein Angebot für die Initialisierung liegt bereits vor (15.000 €). Die Betriebskosten müssen noch verhandelt werden.	Erstes Quartal im Folgejahr	Anschaffung: 15.000 € Betrieb: noch offen	Frau Meyer (Einkauf)