Merkblatt BSI Standard 200-2

Rahmenentscheidung
von Führungsebene für gesamte Organisation

Wie umfassend wird abgesichert?

Basis Absicherung
- Schneller Einstieg in den Sicherheitsprozess
- Nur Basis-Anforderungen (Muss-Anforderungen)
- Gesamte Organisation, aber geringere Tiefe
- Fundament legen, später auf Standard erweitern

Standard Absicherung
- Vollständiger IT-Grundschutz
- Basis- und Standard-Anforderungen
- Gesamte Organisation, volle Tiefe
- Zertifizierungsfähig (ISO 27001 auf Basis IT-Grundschutz)

Kern Absicherung
- Fokus auf "Kronjuwelen" (kritischste Assets)
- Alle Anforderungen, aber nur für ausgewählte Objekte
- Enger Scope, volle Tiefe
- Höchste Priorität zuerst, Rest später nachziehen

Schritt 1
Geltungsbereich festlegen

Was soll geschützt werden?

- Welche IT Systeme?
- Welche Netzwerke ?
- Welche Anwendungen
- Welche Räume?
- Welche Prozesse?

Zu großer Scope = Ressourcenverschwendung
Optimaler Scope
Zu kleiner Scope = Risiken außerhalb des Blickfelds

Schritt 2
Strukturanalyse

Welche Abhängigkeiten gibt es ?

- Schnittstellen
- Datenflüsse
- Zuständigkeiten
- (Gemeinsame) Terminologie

Schritt 3
Schutzbedarfsfeststellung

Einordnung in Schutzziele

- **Vertraulichkeit** „Was passiert, wenn Unbefugte Objekt sehen?"
- **Integrität** „Was passiert, wenn Objekt unbemerkt verändert wird?"
- **Verfügbarkeit** „Was passiert, wenn Objekt ausfällt?"

Einordnung in Schutzbedarfskategorien

Sehr Hoch = Schaden kann existenzbedrohend sein
Hoch = Schaden kann beträchtlich sein
Normal = Schaden ist begrenzt und überschaubar

Schritt 4
Modellierung

Welche Anforderungen gelten?

- **Objekt definieren** Aus Schritt 1-3 z.B.: Server X, mit Abhängigkeit von Netzwerk Y mit sehr hohem Schutzbedarf
- **BSI Baustein verknüpfen** Aus IT-Grundschutz-Kompendium z.B.: SYS.1.1 (Server), APP.3.2 (Webserver), NET.1.1 (Netzwerk)
- **Soll-Katalog erstellen** Liste aller Anforderungen für die gesamte Organisation

Schritt 5
IT-Grundschutz-Check

Soll/Ist-Vergleich
„Sind die Anforderungen des Soll-Katalogs erfüllt?"

- **Ja** Vollständig umgesetzt
- **Teilweise** Noch Lücken vorhanden
- **Nein** Noch nicht erfüllt
- **Entbehrlich** Nicht relevant oder durch Alternative abgedeckt

Schritt 6
Realisierung der Maßnahmen

Maßnahmen zuweisen

- Priorisierung
- Kosten & Budget
- Terminfindung
- Verantwortung
- Schulungen