Schadens- und Risikokategorien gemäß BSI-Standard 200-3

IT-Sicherheit

ITT-Net-IS

10. April 2025

1 Ziel und Hintergrund

Zur Bewertung von Risiken im Kontext der Informationssicherheit empfiehlt das BSI im Rahmen des IT-Grundschutzes eine strukturierte Risikoeinschätzung. Diese erfolgt durch eine Kombination aus der Eintrittswahrscheinlichkeit und der potenziellen Schadenshöhe. Das Ergebnis dient der Einordnung in Risikokategorien, die wiederum als Grundlage für die Auswahl geeigneter Schutzmaßnahmen dienen.

2 Risikoeinschätzung

2.1 Einflussgrößen

Zur Einschätzung eines Risikos werden zwei Hauptdimensionen berücksichtigt:

- ***Eintrittshäufigkeit der Gefährdung***
- ***Potenzielle Schadenshöhe, die bei Eintritt entstehen würde***

Die Kombination dieser beiden Werte ergibt den Risikowert.

2.2 Kategorisierung der Eintrittshäufigkeit

Die Eintrittswahrscheinlichkeit wird in vier qualitative Kategorien eingeteilt:

Eintrittshäufigkeit	Beschreibung
selten	höchstens einmal alle fünf Jahre
mittel	einmal alle fünf Jahre bis einmal jährlich
häufig	einmal jährlich bis einmal monatlich
sehr häufig	mehrmals pro Monat

2.3 Kategorisierung der Schadenshöhe

Auch die Schadenshöhe wird in vier qualitative Kategorien unterteilt:

Schadenshöhe	Beschreibung
vernachlässigbar	geringe Auswirkungen, können ignoriert werden
begrenzt	überschaubare, kontrollierbare Auswirkungen
beträchtlich	erhebliche Auswirkungen auf Organisation oder Prozesse
existenzbedrohend	katastrophale Schäden, ggf. existenzgefährdend

3 Risikobewertung

Basierend auf Eintrittshäufigkeit und Schadenshöhe erfolgt die Einordnung in eine von vier Risikokategorien:

Risiko	Beschreibung
gering	Maßnahmen ausreichend, Risiko kann beobachtet und akzeptiert werden
mittel	Maßnahmen möglicherweise unzureichend
hoch	Schutzmaßnahmen bieten keinen ausreichenden Schutz
sehr hoch	Maßnahmen unzureichend, Risiko in der Praxis kaum akzeptabel

4 Hinweise zur Anwendung

Jede Institution sollte diese Kategorien individuell auf ihre Abläufe abstimmen. Die Beschreibung der Kategorien muss mit den Fachabteilungen abgestimmt werden, um eine einheitliche Einschätzung zu gewährleisten.

5 Beispiel aus der Praxis

5.1 Virtualisierungsserver S1

- **Gefährdung:** Abhören bei Live-Migration (G 0.15)
- **Eintrittshäufigkeit:** selten
- **Schadenshöhe:** beträchtlich
- **Risiko:** mittel

5.2 Datenbank A1

- **Gefährdung:** SQL-Injection (G 0.28)
- **Eintrittshäufigkeit:** häufig
- **Schadenshöhe:** beträchtlich
- **Risiko:** hoch

6 Fazit

Die strukturierte Risikoeinschätzung gemäß BSI 200-3 erlaubt eine nachvollziehbare und vergleichbare Bewertung von Gefährdungen. Sie bildet die Grundlage für risikoorientierte Sicherheitsmaßnahmen und sollte regelmäßig überprüft und angepasst werden.