Risiken einstufen

Häufigkeit und Auswirkungen einschätzen

Die **Höhe eines Risikos** ergibt sich aus der **Häufigkeit einer Gefährdung** und der drohenden **Schadenshöhe**. Ein Risiko ist umso größer, je häufiger eine Gefährdung ist, umgekehrt sinkt es, je geringer der mögliche Schaden ist.
Grundsätzlich können beide Größen sowohl **quantitativ**, also mit genauen Zahlenwerten, als auch **qualitativ**, also mit Hilfe von Kategorien zur Beschreibung der Größenordnung, bestimmt werden. Erfahrungsgemäß sind jedoch hinreichend verlässliche quantitative Angaben, insbesondere zur Häufigkeit von Schadensereignissen im Bereich der Informationssicherheit, so gut wie nicht vorhanden und auch dort, wo es verlässliche Statistiken gibt, sind daraus abgeleitete exakte Prognosen auf zukünftige Ereignisse problematisch, wenn nicht gar unmöglich. Daher **empfiehlt** sich ähnlich wie bei der Schutzbedarfsfeststellung ein **qualitativer Ansatz** mit einer begrenzten Anzahl an Kategorien.

Nachfolgend als Beispiel ein Vorschlag aus dem BSI-Standard 200-3 für ein mögliches vierstufiges Klassifikationsschema zur Bewertung von **Eintrittshäufigkeiten**.

Eintrittshäufigkeit	Beschreibung
selten	Das Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre auftreten.
mittel	Das Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Das Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
Sehr häufig	Das Ereignis tritt mehrmals im Monat ein.

Auch für die Klassifikation möglicher **Schadensauswirkungen** enthält der BSI-Standard als Beispiel ein vierstufiges Klassifikationsschema.

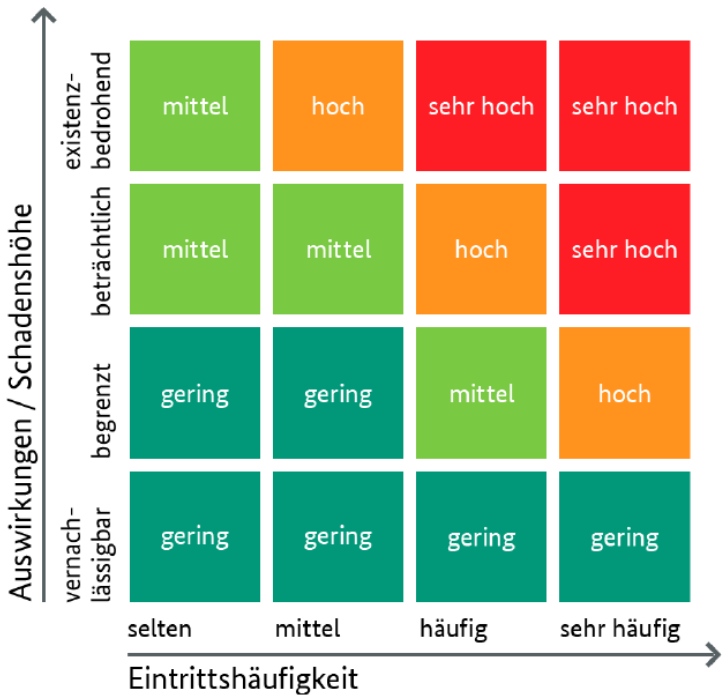
Schadenshöhe	Schadensauswirkungen
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen.

Risiko bewerten

Nachdem Sie die Eintrittshäufigkeiten und Schadensauswirkungen einer Gefährdung eingeschätzt haben, können Sie das aus beiden Faktoren **resultierende Risiko bewerten**. Der BSI-Standard 200-3 enthält ein Beispiel mit vier Stufen, dass Sie an die Gegebenheiten und Erfordernisse Ihrer Institution anpassen können. Die folgende Tabelle ist an dieses Beispiel angelehnt.

Risikokategorie	Definition
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen bieten einen ausreichenden Schutz.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer großen Wahrscheinlichkeit nicht akzeptiert werden.
Sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer sehr großen Wahrscheinlichkeit nicht akzeptiert werden.

Zur Darstellung von Eintrittshäufigkeiten, Schadensauswirkungen und Risiken ist eine Risikomatrix ein gebräuchliches und sehr anschauliches Instrument. Auch hierzu enthält der BSI-Standard 200-3 einen Vorschlag, den Sie an die Festlegungen Ihrer Institution zur Risikobewertung anpassen können.



Aufgabenstellung

- **Erstellen** Sie eine **Risikobewertung** für den Virtualisierungsserver S001!
  - **Nutzen** Sie dazu die Vorlage „**Vorlage_Risiko_einstufen_ServerS001**“!
  - **Kopieren** Sie sich diese Vorlage und **benennen** Sie das Dokument entsprechend um!
  - **Informieren** Sie sich mithilfe des **Interviews** (Dokument: **Auszug_Interviews**) über die Situation im Krankenhaus!
  - **Vervollständigen** Sie anschließend die Tabelle mit Inhalten in den Spalten **Eintrittswahrscheinlichkeit**, **Schadenshöhe** und der daraus folgenden **Risikokategorie**!