



Ist die Gefährdung relevant?

Sollten hingegen einzelne oder mehrere Zielobjekte aus der Strukturanalyse im Rahmen der Modellierung nicht mit einem Baustein verknüpft worden sein, ist jede elementare Gefährdung dahingehend zu bewerten, ob diese direkt, indirekt oder gar nicht auf das Zielobjekt einwirken kann:

- „Direkt relevant“ bedeutet, dass die jeweilige Gefährdung auf das betrachtete Zielobjekt einwirken kann und deshalb im Rahmen der Risikoanalyse behandelt werden muss.
- Indirekt relevant“ bedeutet, dass die jeweilige Gefährdung zwar auf das betrachtete Zielobjekt einwirken kann, in ihrer potenziellen Wirkung aber nicht über andere elementare Gefährdungen hinausgeht. In diesem Fall muss die jeweilige Gefährdung für dieses Zielobjekt nicht gesondert im Rahmen der Risikoanalyse behandelt werden.
- „Nicht relevant“ bedeutet, dass die jeweilige Gefährdung nicht auf das betrachtete Zielobjekt einwirken kann und deshalb im Rahmen der Risikoanalyse nicht behandelt werden muss.

Wie ist die Auswirkung?

Persönlich bin ich bei der Bewertung der Auswirkungen mit einer zweistufigen Bewertungsskala in der Vergangenheit sehr gut gefahren. Die beiden Stufen haben sich wie folgt unterschieden.

- vernachlässigbar / gering
 - Aus dem Eintritt des Risikos entsteht kein Schaden oder der resultierende Schaden ist so gering, dass er zusätzliche Aufwände für die Risikobehandlung nicht rechtfertigt.
- Erheblich
 - Der Eintritt des Risikos hat beträchtliche Auswirkungen. Ein Eintritt des Risikos ist durch eine geeignete Risikobehandlung zu verhindern.

Wie wird das Risiko bewertet?

Persönlich bin ich mit einer zweistufigen Bewertungsskala in der Vergangenheit sehr gut gefahren. Die beiden Stufen unterscheiden sich wie folgt.

- tragbar
 - Das Risiko liegt im Rahmen der für einen IT-Betrieb unvermeidlichen Basisrisiken. Es erfordert keine Maßnahmen zur Risikobehandlung.
- untragbar
 - Das Risiko geht über die für einen IT-Betrieb unvermeidlichen Basisrisiken hinaus und erfordert eine geeignete Risikobehandlung. Risiken werden als untragbar bewertet, wenn ihre Eintrittswahrscheinlichkeit „nicht ausschließen/wahrscheinlich“ und ihre Auswirkungen „erheblich“ sind.

Ist der Eintritt wahrscheinlich?

Persönlich bin ich mit einer zweistufigen Bewertungsskala in der Vergangenheit sehr gut gefahren. Die beiden Stufen unterscheiden sich wie folgt.

- ausschließen / unwahrscheinlich
 - Ein Eintritt des Risikos ist entweder auszuschließen oder so unwahrscheinlich, dass damit im Betrieb nicht gerechnet werden muss.
- nicht ausschließen / wahrscheinlich
 - Mit dem Eintreten des Risikos muss realistisch gerechnet werden.

Wie hoch ist der Schaden?

Persönlich bin ich mit einer Bewertungsskala aufbauend auf den bereits definierten Schadenshöhen der Schutzbedarfskategorien in der Vergangenheit sehr gut gefahren. Als kleine Erinnerung, wie der Schutzbedarf ermittelt wurde, habe ich die entsprechende Passage hier noch einmal aufgeführt. Der Schutzbedarf ist meist nicht quantifizierbar, daher beschränkt sich der BSI IT-Grundschatz somit auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird. Die nachfolgenden Schritte erläutern, wie für Geschäftsprozesse und die mit diesen verbundenen Anwendungen jeweils die adäquate Schutzbedarfskategorien ermittelt werden können. Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

- Verstoß gegen Gesetze/Vorschriften/Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Schutzbedarfskategorien

- Normal
 - Die Schadensauswirkungen sind begrenzt und überschaubar. Der finanzielle Schaden beläuft sich auf ≤€€.
- Hoch
 - Die Schadensauswirkungen können beträchtlich sein. Der finanzielle Schaden beläuft sich auf ≤€€€€.
- Sehr hoch
 - Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen. Der finanzielle Schaden beläuft sich auf ≥€€€€€.