Kapitel 4: Schutzbedarfsfeststellung

4.1 Überblick

Wie viel Schutz benötigen der betrachtete Informationsverbund und die ihm zugehörigen Objekte? Wie kommen Sie zu begründeten und nachvollziehbaren Einschätzungen des Schutzbedarfs? Welche Objekte benötigen mehr Sicherheit, bei welchen genügen elementare Schutzmaßnahmen?

Ziel der **Schutzbedarfsfeststellung** ist es, diese Fragen zu klären und damit die **Auswahl angemessener Sicherheitsmaßnahmen** für die einzelnen Objekte des betrachteten Informationsverbundes zu steuern.

Die Schutzbedarfsfeststellung

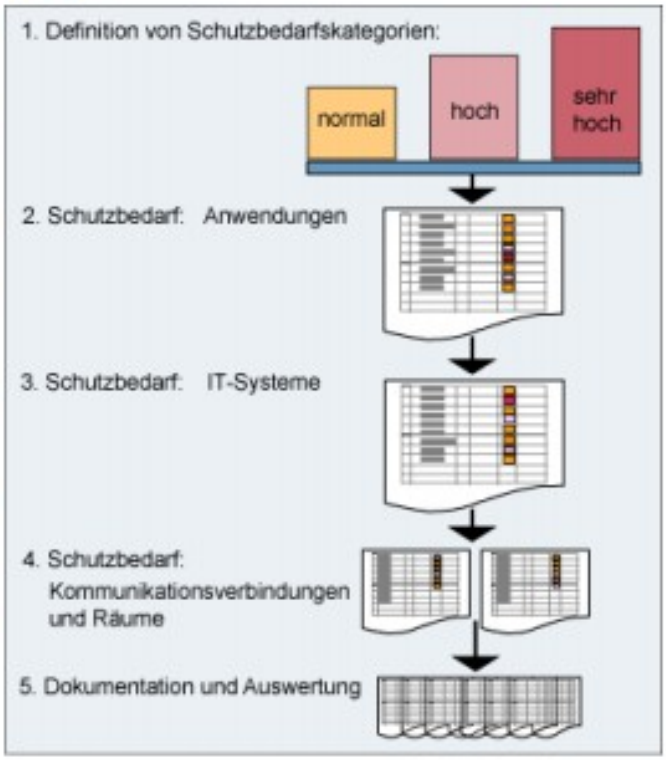
- sensibilisiert die Institution in Bezug auf Informationssicherheit,
- schafft eine einheitliche Sicherheitsdefinition und ein abgestimmtes Sicherheitsverständnis zwischen den Zuständigen,
- erleichtert die Auswahl der IT-Grundschutz-Maßnahmen und
- identifiziert Komponenten, für die eventuell höherwertige Maßnahmen erforderlich sind.

Die Entscheidungen zur Schutzbedarfsfeststellung sollten nachvollziehbar dokumentiert werden und die Zustimmung aller Beteiligten finden, insbesondere auch des Managements.

Was gehört zu einer Schutzbedarfsfeststellung?

Zur Schutzbedarfsfeststellung gehören die folgenden Aktivitäten:

1. die auf Ihre Organisation zugeschnittene Definition der Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“,
2. die Feststellung des Schutzbedarfs der Anwendungen, die in der Strukturanalyse erfasst wurden, mit Hilfe der definierten Kategorien,
3. die Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen,
4. daraus abgeleitet die Feststellung des Schutzbedarfs der Kommunikationsverbindungen und Räume sowie
5. die Dokumentation und Auswertung der vorgenommenen Einschätzungen.



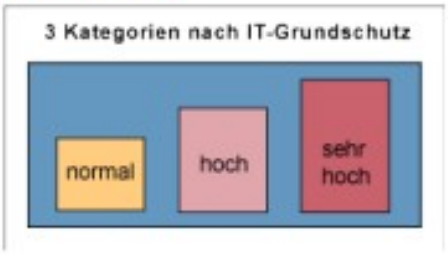
4.2 Schutzbedarfskategorien

4.2.1 Definition

Der Schutzbedarf eines Objekts orientiert sich an dem Ausmaß der **Schäden**, die entstehen können, wenn seine Funktionsweise beeinträchtigt ist. Da die Höhe eines Schadens häufig nicht genau bestimmt werden kann, sollten Sie eine für Ihren Anwendungszweck passende Anzahl von Kategorien definieren, anhand derer Sie den Schutzbedarf unterscheiden.

Die IT-Grundschutz-Vorgehensweise empfiehlt **drei Schutzbedarfskategorien**:

- **normal:** Die Schadensauswirkungen sind begrenzt und überschaubar.
- **hoch:** Die Schadensauswirkungen können beträchtlich sein.
- **sehr hoch:** Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.



Schutzziele und Grundwerte

Bei der Schutzbedarfsfeststellung ist danach zu fragen, welcher Schaden entstehen kann, wenn die **Grundwerte** Vertraulichkeit, Integrität oder Verfügbarkeit eines Objekts verletzt werden, wenn also

- vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der **Vertraulichkeit**),
- die Korrektheit der Informationen und der Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der **Integrität**),
- autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der **Verfügbarkeit**).

4.2.2 Abgrenzung der Schutzbedarfskategorien

Wann hat ein Objekt einen normalen, wann einen hohen und wann einen sehr hohen Schutzbedarf?

Eine allgemeingültige Antwort auf diese Frage ist nicht bei allen Schadensszenarien möglich. Eine erste Abgrenzung der Kategorien finden Sie in Kapitel 4.3 des BSI-Standards 100-2. Die dort angeführten relativ allgemein gehaltenen Definitionen können Sie als Ausgangspunkt nehmen und an die besonderen Gegebenheiten Ihrer Organisation anpassen und gegebenenfalls ergänzen.

Beispielsweise finden Sie dort für die Schutzbedarfskategorie „normal“ und das Schadensszenario „finanzielle Auswirkungen“ die Festlegung:

- „Der finanzielle Schaden bleibt für die Institution tolerabel.“

Was aber heißt für ein Unternehmen „tolerabel“? Für ein sehr großes Unternehmen spielen einige Millionen Euro mehr oder weniger vielleicht keine große Rolle, kleinere und mittlere Unternehmen kann ein Schaden in dieser Höhe dagegen zum Bankrott bringen. Bei der Abgrenzung der Schadenskategorien müssen Sie also die Besonderheiten der betrachteten Institution berücksichtigen, zum Beispiel

- in Bezug auf das Szenario „finanzielle Auswirkungen“ die Höhe des Umsatzes oder des Gewinns eines Unternehmens oder die Höhe des bewilligten Budgets einer Behörde,
- in Bezug auf das Szenario „Beeinträchtigung der Aufgabenerfüllung“ das Vorhandensein von Ausweichverfahren bei einem Ausfall eines IT-gestützten Verfahrens.

4.2.3 Schutzbedarf und Schutzziele

Da der Schutzbedarf für die Grundwerte **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** unterschiedlich hoch sein kann und als Konsequenz unterschiedliche Sicherheitsmaßnahmen erforderlich sind, müssen Sie den Schutzbedarf für alle drei Ziele gesondert betrachten.

Der Schutzbedarf einer Firmendarstellung auf einem öffentlichen Webserver ist beispielsweise aus Sicht der **betreffenden Firma**

- bezüglich des Schutzziels Vertraulichkeit nicht relevant, da die Firmendarstellung ausschließlich Informationen enthält, die das Unternehmen sowieso an die Öffentlichkeit bringen will,
- bezüglich des Schutzziels Integrität in der Regel im normalen Bereich, da sich Integritätsverletzungen leicht erkennen und korrigieren lassen und der Image-Verlust, der sich z. B. aus einer gefälschten Homepage ergibt, meistens nicht nachhaltig ist,
- bezüglich des Schutzziels Verfügbarkeit ebenfalls als normal einzuschätzen, es sei denn, aus der fehlenden Verfügbarkeit resultieren gravierende wirtschaftliche Folgen, z. B. weil die Angebote der Firma nicht mehr von den Kunden wahrgenommen werden.

Sollte die Firmendarstellung auf dem Rechner eines **Providers** angesiedelt sein, könnte sich aus dessen Sicht bezüglich Integrität und Verfügbarkeit ein höherer Schutzbedarf ergeben, da er im Schadensfall seine Verpflichtungen nachweisbar nicht angemessen erfüllt hat und somit gravierende finanzielle Verluste befürchten muss, da zum Beispiel der Kunde den Vertrag kündigen könnte.

Wie dieses Beispiel zeigt, kann der Schutzbedarf für die Grundwerte unterschiedlich hoch sein. Für die gleiche Anwendung kann der Schutzbedarf auch unterschiedlich eingeschätzt werden, je nachdem aus welcher Sicht er betrachtet wird.

Bei der Abschätzung des Schadens sollten Sie unbedingt die Verantwortlichen und die Benutzer der Anwendung einbeziehen. Diese wissen meist sehr genau, welche Schäden bei falschen Daten oder bei einem Ausfall einer Anwendung auftreten. Es ist trotzdem möglich, dass der Schutzbedarf von den Mitarbeitern (und auch innerhalb der Projektgruppe) unterschiedlich eingeschätzt wird. Falls kein Konsens erzielt werden kann, muss das Management entscheiden.