Definition Schutzbedarfskategorien

Der Schutzbedarf wird im IT-Grundschutz in folgende drei Kategorien unterteilt:

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

Es kann für Institution auch sinnvoll sein, weitere Kategorien zu definieren. Beispielsweise kann eine Abstufung **„unkritisch“** nach unten eingeführt werden. Diese könnte wie folgt definiert sein: „Schadensauswirkungen sind nicht oder nur sehr minimal vorhanden“.
Werden nur ein oder zwei Kategorien genutzt, ist die damit erreichbare Abstufung meist nicht granular genug. Werden dagegen fünf oder mehr Schutzbedarfskategorien verwendet, ist eine klare Unterscheidung zwischen den einzelnen Stufen schwieriger.

Der Schaden, der von einer **Verletzung der Grundwerte** (Vertraulichkeit, Integrität, Verfügbarkeit) ausgehen kann, kann sich auf verschiedene **Schadensszenarien** beziehen:

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
- Beeinträchtigungen der persönlichen Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung oder
- finanzielle Auswirkungen.

Zur Orientierung, welchen Schutzbedarf ein potenzieller Schaden und seine Folgen erzeugen, dienen die Tabellen auf Seite 3 und 4. Für alle Schäden, die sich nicht in diese Szenarien abbilden lassen, muss ebenfalls eine Aussage getroffen werden, wo die Grenzen zwischen „normal“, „hoch“ oder „sehr hoch“ zu ziehen sind. Bei der **Abgrenzung der Schadenskategorien** müssen Sie immer die **Besonderheiten der betrachteten Institution berücksichtigen** und diese individuell anpassen. Häufig treffen für einen Schaden mehrere Schadensszenarien zu. So kann beispielsweise der Ausfall einer Anwendung die Aufgabenerfüllung beeinträchtigen, was direkte finanzielle Einbußen nach sich zieht und gleichzeitig auch zu einem Imageverlust führt. Wie wichtig ein Szenario jeweils ist, unterscheidet sich von Institution zu Institution.

Aufgabenstellung:

Beantworten Sie folgende Fragen!

Beschreiben Sie die drei Schutzbedarfskategorien, die vom IT-Grundschutz vorgeschlagen werden!

Normal, Hoch, Sehr Hoch

Beschreiben Sie, wieso es problematisch ist, wenn es mehr oder weniger als drei Schutzbedarfskategorien gibt?

Bei weniger als 3 ist die Unterscheidung nicht granular genug

Bei mehr als 5 ist es schwer die Grenzen zwischen den Kategorien zu definieren

Nennen Sie drei Schadensszenarien, die für das Krankenhaus bzw. für die Abrechnungsabteilung relevant sind!

Finanzielle Auswirkung

Beeinträchtigung der Aufgabenerfüllung

Beeinträchtigung des informationellen Selbstbestimmungsrechts

Bestimmen und beschreiben Sie für ein gewähltes Schadenszenarien eine individuelle Abgrenzung zwischen den drei Schutzbedarfskategorien (sehr hoch, hoch, normal)!

Tipp: Nutzen Sie dazu den Anhang auf Seite 3 und 4!

Programme funktionieren nicht für 12 Stunden:

Schutzbedarfskategorie Normal, da der Ausfall nicht länger als 24 Stunden bzw. 72 Stunden liegt

Finanzieller Schaden:

normal < 25.000

hoch < 250.000

sehr hoch > 250.000

Anhang: Abgrenzung der Schutzbedarfskategorien

Schutzbedarfskategorie: normal

1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Schutzbedarfskategorie: hoch

1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nichtabsolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeitliegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Schutzbedarfskategorie: sehr hoch

1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.