Lizenzbestimmungen

Diese Vorgabe definiert Maßnahmen der Kategorie „C“. Maßnahmen der Kategorie „C“ müssen behandelt werden. Sie sind prinzipiell verpflichtend (Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT/DÜRFEN KEINE, siehe Abschnitt 1.2 T3) und ihre Behandlung wird bei einem Audit geprüft.

Für Maßnahmen der Kategorie „C“ besteht die Möglichkeit, in Eigenverantwortung geeignete, verhältnismäßige und wirksame (siehe §30 Abs. 1 Satz 1 BISG n.F.) Formen der Umsetzung zu entwickeln:

- IT-Systeme der Schutzkategorie „nachrangig“ können von der Implementation der Maßnahmen der Kategorie „C“ pauschal ausgenommen werden (siehe Anhang A.2.5 E3).
- Maßnahmen der Kategorie „C“ müssen nur bei jenen IT-Ressourcen umgesetzt werden, die dazu technisch in der Lage sind. Schutzmaßnahmen der Kategorie „C“ setzen auf der vorhandenen IT-Infrastruktur auf; für die Umsetzung werden keine Neuanschaffungen von Soft- oder Hardware verlangt.
- Wenn bei betroffenen IT-Ressourcen eine Maßnahme der Kategorie „C“ technisch nicht umgesetzt werden kann, empfiehlt die VdS 10100, die dadurch entstehende Schwachstelle in das Risikomanagement (siehe Anhang A.2) aufzunehmen:
    - Der Untersuchungsgegenstand der Risikoidentifikation, -analyse und -behandlung sind jene IT-Ressourcen, die die Maßnahme technisch nicht (vollständig) umsetzen können.
    - Die fehlende Umsetzung der Maßnahme wird bei der Risikoidentifizierung (siehe Anhang A.2.3) als Schwachstelle betrachtet. Die zu untersuchende Fragestellung lautet: „Welche Risiken entstehen, weil die betroffenen IT-Ressourcen X technisch nicht dazu in der Lage sind, die Maßnahme Y (vollständig) umzusetzen?“
    - Diese Vorgehensweise soll die Sensibilisierung der Beteiligten erhöhen und schließlich eine Eindämmung der bestehenden Risiken erreichen.
- Auch für jene IT-Ressourcen, die technisch dazu in der Lage sind eine Maßnahme der Kategorie „C“ umzusetzen, besitzt die Organisation Entscheidungsfreiheit. Die Organisation darf frei entscheiden, bei welchen IT-Ressourcen eine Maßnahme der Kategorie „C“ vollständig umgesetzt wird, bei welchen IT-Ressourcen die Umsetzung nur teilweise erfolgt und bei welchen IT-Ressourcen sie komplett unterbleibt - die Organisation darf für jede Maßnahme der Kategorie „C“ den Geltungsbereich und den Implementierungsgrad frei wählen.
- Wenn sich die Organisation bewusst gegen die (vollständige) Umsetzung einer Maßnahme der Kategorie „C“ entscheidet, gilt:
    - Die Organisation muss ihre Entscheidung nicht begründen oder dokumentieren.
    - Sie ist dazu verpflichtet, die dadurch entstehende Schwachstelle in das Risikomanagement (siehe Anhang A.2) aufzunehmen. Der Untersuchungsgegenstand der Risikoidentifikation, -analyse und -behandlung sind jene IT-Systeme, bei denen die Maßnahme nicht oder nicht vollständig umgesetzt wird, obwohl sie dazu technisch in der Lage wären. Die zu untersuchende Fragestellung lautet: „Welche Risiken entstehen weil Maßnahme X nicht bzw. nicht vollständig umgesetzt wird, obwohl dies technisch möglich wäre?“ Durch die Risikoidentifizierung und -analyse wird systematisch ermittelt, welche Risiken die Organisation durch ihre Entscheidung in Kauf nimmt. Im Zuge der Risikobehandlung muss sie „geeignete, verhältnismäßige und wirksame Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken“ definieren, dokumentieren und umsetzen (siehe Anhang A.2.5 A2). Dabei besteht die Möglichkeit, Risiken zu akzeptieren, wenn ihre Schadenhöhen und/oder Eintrittswahrscheinlichkeiten unterhalb der Risikoakzeptanzgrenze liegen (siehe Anhang A.2.5 E3) oder wenn dies vom Topmanagement gewollt ist (siehe Anhang A.2.5 A5).
- Maßnahmen dieser Kategorie sind in der ersten Spalte der Tabellen mit dem Buchstaben „C“ gekennzeichnet (z. B. „C1“ oder „C2.5“).