Lizenzbestimmungen

- Die in der VdS 10100 geforderten Dokumentationen setzen (zusammen mit weiteren Dokumenten wie die IS-Leitlinie, den IS-Richtlinien, den für die Informationssicherheit relevanten Verfahren und weiteren geforderten Dokumenten sowie den Dokumenten, die im Zuge des Betriebs des ISMS und im Zuge der kontinuierlichen Verbesserung und Anpassung entstehen) die Dokumentationspflichten von § 30, Abs. 1, Satz 1 und 3 BSIG n.F. („(Betroffene) Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, (…) zu ergreifen, um Störungen der (Informationssicherheit) zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.“) um.
- Die folgenden Maßnahmen der VdS 10100 verpflichten die Organisation zum Führen einer Dokumentation:
  - Abschnitt 1.3.1 A1.2:
    Das Ergebnis der Prüfung ob die Organisation als „wichtige“ oder „besonders wichtige“ Einrichtung im Sinne von § 28 BSIG n.F. gilt muss zusammen mit seiner Begründung dokumentiert werden.
  - Abschnitt 4.2.2 A1:
    Verantwortlichkeiten für die Informationssicherheit (siehe Abschnitte 4.3 bis 4.13) müssen eindeutig und widerspruchsfrei zugewiesen werden. Für jede Zuweisung müssen verschiedene Punkte dokumentiert werden.
  - Abschnitt 4.2.3 A2.3:
    In der Dokumentation der Verantwortlichkeiten (siehe Abschnitt 4.2.2) müssen nicht durchgeführte Funktionstrennung besonders hervorgehoben und begründet werden.
  - Abschnitt 6.3 E1:
    Wenn Ausnahmen von Richtlinien etabliert werden, müssen sie im Vorfeld genehmigt und dokumentiert werden.
  - Abschnitt 8.3 A1.6:
    Inhalte der Schulungs- und Sensibilisierungsmaßnahmen und die Teilnahme an ihnen müssen dokumentiert werden.
  - Abschnitt 9.2 A1:
    Die Organisation muss ihre zentralen Prozesse und ihre Prozesse mit hohem Schadenpotenzial dokumentieren.
  - Abschnitt 9.3 A1:
    Die Organisation muss ihre wichtigen IT-Ressourcen ermitteln und dokumentieren.
  - Abschnitt 9.4 A1:
    Die Organisation muss ermitteln, ob sie kritische Informationen verarbeitet, überträgt und/oder speichert und diese dokumentieren.
  - Abschnitt 9.5 A1:
    Die Organisation muss - falls vorhanden - ihre kritischen IT-Ressourcen dokumentieren.
  - Abschnitt 10.3.1 A1.4:
    Bei Inbetriebnahme von IT-Systemen wird die Durchführung der dafür vorgeschriebenen Arbeitsschritte dokumentiert.
  - Abschnitt 10.3.2 A1.4: Bei Ausmusterung von IT-Systemen wird die Durchführung der dafür vorgeschriebenen Arbeitsschritte dokumentiert.
  - Abschnitt 10.6.1 B1:
    Für jedes wichtige IT-System muss eine Dokumentation der administrativen Tätigkeiten vorhanden sein.
  - Abschnitt 11.4 A2.1:
    Die sicherheitsrelevanten Einstellungen der Schnittstellen zu weniger oder nicht vertrauenswürdigen Netzen müssen dokumentiert werden.
  - Abschnitt 14.4.2 B2:
    Eine schriftliche Dokumentation von Änderungen in Verträgen muss mit den Lieferanten

von wichtigen externen IT-Ressourcen vereinbart werden.
    - Abschnitt 15.2 A1.6:
      Das Anlegen und Ändern von Zugängen, Zugriffsrechten und Zutrittsrechten sowie für das Zurücksetzen von Authentifizierungsmerkmalen muss dokumentiert werden.
    - Abschnitt 16.3 A1.7:
      Die Durchführung und die Ergebnisse der Tests der Datensicherung und -wiederherstellung müssen dokumentiert werden.
    - Abschnitt 17.3 A2:
      Die Organisation muss prüfen, welche Maßnahmen notwendig sind, um mögliche Sicherheitsvorfälle und Schwachstellen erkennen zu können. Das Ergebnis der Prüfung muss zusammen mit seiner Begründung dokumentiert werden.
    - Abschnitt 17.4 A1.4:
      Im Zuge der Reaktion auf Sicherheitsvorfälle müssen der Sicherheitsvorfall und der Schaden so dokumentiert werden, dass die Organisation ihre Informationspflichten erfüllen und den Sicherheitsvorfall nachbereiten kann.
    - Abschnitt 17.5.2 B1:
      Die Abhängigkeiten der wichtigen IT-Ressourcen untereinander müssen dokumentiert und dabei die Reihenfolge ihrer Wiederherstellung festgelegt werden.
    - Abschnitt 18.3 A1.9:
      Im Zuge der Bewältigung einer IT-Krise muss die Entwicklung der IT-Krise, die Reaktionen auf sie und der entstandene Schaden muss so dokumentiert, dass die Organisation ihre Informationspflichten erfüllen und die IT-Krise nachbereiten kann.
    - Abschnitt 18.4 B5:
      Die Durchführung und die Ergebnisse des jährlichen Tests eines der Verfahren für das Reagieren auf die wahrscheinlichsten IT-Krisen müssen dokumentiert werden.
    - Anhang A.1 A2.2:
      Alle Verfahren müssen in einer für die jeweilige Zielgruppe zugänglichen und verständlichen Form dokumentiert und bekannt gegeben.
    - Anhang A.2.3 A1.1:
      Die Durchführung und die Ergebnisse von Risikoidentifizierungen müssen dokumentiert werden.
    - Anhang A.2.4 A1.1:
      Die Durchführung und die Ergebnisse von Risikoanalysen müssen dokumentiert werden.
    - Anhang A.2.5 A2:
      Die Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der identifizierten Risiken müssen definiert, dokumentiert und umgesetzt werden.
- Die folgenden Maßnahmen der VdS 10100 empfehlen eine Dokumentation:
    - Abschnitt 10.2 E2:
      Die VdS 10100 empfiehlt eine Dokumentation zu führen, in der Besonderheiten der Installation und Konfiguration der IT-Systeme verzeichnet sind.
    - Abschnitt 14.3 E1.6:
      Die VdS 10100 empfiehlt, in den Verträgen mit Lieferanten externer IT-Ressourcen Dokumentationspflichten aufzunehmen.
    - Abschnitt 16.3 E4:
      Die VdS 10100 empfiehlt, die Datensicherung und -wiederherstellung so zu dokumentieren, dass Mitarbeiter die geforderten Tests anhand der vorliegenden Dokumentation durchführen können.
- Die VdS 10100 legt nicht fest, in welchem Format die von ihr geforderten Dokumentationen vorliegen oder mit welchen Hilfsmitteln sie erstellt und gepflegt werden müssen, was der umsetzenden Organisation großen Gestaltungsspielraum gibt.
    - Zu Beginn eines Umsetzungsprojekts sollten die Vorgehensweisen und technischen

Hilfsmittel für die Erstellung und Pflege von Dokumentationen verbindlich verabredet werden. Dabei sollten die Personen, die für die jeweilige Dokumentation verantwortlich sind, in den Entscheidungsprozess eingebunden werden. Bei der Auswahl sollten bereits vorhandenen Lösungen bevorzugt werden, um Redundanzen oder gar widersprüchliche Lösungen innerhalb der Organisation zu vermeiden.

  - Wenn die technischen Hilfsmittel für das Erstellen und Pflegen von Dokumentationen frei gewählt werden können sollte der Aufbau eines zentralen Wikis für die Umsetzung der VdS 10100 geprüft werden. Ein Wiki bietet viele Vorteile (wie z. B. die erzwungene zentralisierte Datenhaltung, die integrierte Volltextsuche, die Möglichkeit der einfachen Verlinkung mit internen und externen Quellen oder die eingebaute Versionshistorie) und eignet sich prinzipiell dazu, alle von der VdS 10100 geforderten Dokumente (wie z. B. die IS-Leitlinie, die IS-Richtlinien, die für die Informationssicherheit relevante Verfahren, die Inventarisierung, der Netzwerkplan und sämtliche Dokumentationen) zu verwalten.

- Die in der VdS 10100 geforderten Dokumentationen sind ein Bestandteil der IS-Aufzeichnungen. Sie müssen über die Richtlinie „Aufbau und Funktionsweise des ISMS“ (siehe Abschnitt 6.4) auffindbar sein.