

Control 1.3.2: Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?

Eine der MUSS-Anforderungen dieses Controls lautet:

„Die für die Organisation kritischen Informationswerte sind identifiziert und erfasst.“

Häufig interpretieren Unternehmen diese Anforderung als Verzeichnis ihrer physischen Assets. In manchen Fällen geht man sogar davon aus, ein Auszug aus der Anlagenbuchhaltung würde genügen.

In der Vorgängerversion des VDA ISA suggerierte der alte Name des Controls „8.1 Inventarverzeichnis“ dieses Missverständnis möglicherweise noch deutlicher. Doch das reicht bei Weitem nicht aus, um diese Anforderung zu erfüllen.

Zunächst einmal gilt es, das Verständnis des Begriffs „Asset“ oder zu Deutsch „Wert“ in diesem Zusammenhang zu schärfen. Information Assets (= Informationswerte) umfassen alle schutzbedürftigen Unternehmenswerte, Prozesse oder Informationen. Diese Informationen können in physischer (z.B. Dokumente, Prototypen) und/oder digitaler Form (z.B. als Datei oder in Datenbanken) vorliegen. Diese Informationswerte werden auch als „primäre Assets“ bezeichnet. Jede Organisation sollte die Werte und Kritikalität der eigenen Informationen (z. B. Geschäftsgeheimnisse, kritische Geschäftsprozesse, Know-How, Patente, OEM-Daten) kennen.

Dafür gilt es, diese Information Assets zunächst zu identifizieren. Bei der initialen Analyse empfiehlt es sich zunächst in größeren „Clustern“ zu denken, später kann man diese Cluster weiter herunterbrechen. Für jedes Information Asset sollte auch gleich ein Verantwortlicher definiert werden.

Beispiele:

- HR-Informationen (verantwortlich: HR-Manager)
- Finanzdaten (verantwortlich: CFO)
- Vertriebsdaten (verantwortlich: Vertriebschef)
- CAD-Daten / Konstruktionsdaten (verantwortlich: Entwicklungsvorstand)
- und so weiter.

Weiter heruntergebrochen sähe das am Beispiel „HR-Informationen“ so aus:

- Bewerberdaten
- Vergütungsdaten (z.B. Basisgehalt, Zulagen, ergänzende Zahlungen)
- Zeitdaten (z.B. An-/ Abwesenheiten, Urlaubskontingent)
- Stammdaten (z.B. Adresse, Alter, Geschlecht, Bankverbindung, Personalnummer)
- Beschäftigungsdaten
- Abrechnungsdaten (z.B. Basisbezüge, Sozialversicherungsnummer, Steueridentifikationsnummer, Sozialversicherungsstatus)
- Entgeltplanungsdaten
- Leistungsbeurteilung, etc.

Neben den Informationswerten (primären Assets) gibt es die sogenannten Informationsträger (= unterstützende Werte), auf denen die primären Werte verarbeitet werden. Dies sind zum einen die physischen Assets, die wir am Anfang betrachtet hatten (Hardware wie Server, Notebooks, Speichermedien), aber auch Datenbanken, Applikationen oder Archive. Im Gegensatz zu den Informationswerten liegt hier oftmals die Verantwortung bei der IT-Abteilung.

Alle Informationsträger lassen sich den Informationswerten zuordnen.

Diese erweiterte Sichtweise - die Informationswerte und Informationsträger gleichermaßen zu identifizieren und zu erfassen - bildet die Grundlage, ausgehend von der Datenklassifizierung, geeignete Schutzmaßnahmen für die Informationsträger zu definieren. Jeder Informationswert (bzw. jeder Informationscluster) sollte daher durch den jeweiligen Verantwortlichen in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität bewertet werden. Aus dieser Analyse ergeben sich die Basisanforderungen an die IT.