Verwaltung der Werte

Jedes Unternehmen besitzt Werte (Englisch: Assets), die es zu schützen gilt. Das Kapitel A.8 nimmt sich diesem Thema an und verlangt, dass diese Werte identifiziert und angemessene Verantwortlichkeiten zum Schutz definiert werden.

In einem ersten Schritt gilt es, alle Werte zu erfassen. Idealerweise werden diese in Kategorien gesammelt. Dies könnten beispielsweise sein:
- Arbeitsplatz-Rechner, Laptops
- Archive
- Büroräume
- Back-up
- Betriebssysteme
- Daten
- Datenbanken
- Datenträger
- Dokumentationen
- Drucker
- Fahrzeuge
- Klimaanlage
- Kommunikationsverbindungen
- Mobiltelefone, Tablets
- Netzwerk-Geräte
- Protokolle, Korrespondenz
- Schlüssel
- Schränke
- Server
- Serverräume
- Software
- Stromversorgung
- Telefonie

Wichtig ist, dass das Inventar immer aktuell ist. Dazu muss ein entsprechender Prozess etabliert werden, der beim Kauf/Beschaffen anfängt und mit der Ausserbetriebnahme/Zerstörung endet. Einige Unternehmen greifen auf die Anlagenbuchhaltung zurück. Vermutlich wird dies nicht immer ausreichen, ist in der Anlagenbuchhaltung oft nur «Laptop» mit einem Betrag vorhanden. Dies ist als Inventar zu ungenau. Zudem wird jedes Jahr etwas vom entsprechenden Betrag abgeschrieben und eine Rückverfolgung ist sehr schwer. Zusätzlich kann das Inventar gleich auch benutzt werden, wenn einmal ein Gerät in die Reparatur geht. Dies kann in einem entsprechenden Tool gut nachgeführt werden. Für die Risikoanalyse (siehe Maschinenbau 8/18, ab Seite 26) genügt aber die obenstehende Auflistung der Kategorien.

Jeder Wert muss in der Folge seinen Zuständigen sowie eine Klassifizierung enthalten.

Zuständigkeiten

Wie erwähnt, muss für jeden Wert eine verantwortliche Person definiert werden. Dies kann ein Name sein, aber auch eine Rolle. Ich empfehle hier klar eine Rolle. Sollte eine Person das Unternehmen verlassen, muss sonst daran gedacht werden, auch die entsprechenden Werte auf die neue Person umzutragen. Erfahrungsgemäss geht dies gerne vergessen. Die Norm erwähnt explizit, dass diese Rolle nicht im juristischen Sinn Eigentümerin des Werts sein muss. Die Verantwortung für diesen Wert sollte über den gesamten Lebenszyklus gelten. Bei komplexen Informationssystemen ist es zudem erlaubt, eine Gruppe zu bilden und nicht jedes Element einzeln einer Rolle zuzuweisen. Weiter gehören regelmässige Kontrollen mit dazu (in vielen Betrieben kennt man die Inventur als eine Möglichkeit). Diese Aufgabe darf delegiert werden, nicht aber die Verantwortung für diese Tätigkeit.

Zulässiger Gebrauch/Handhabung

Jedes Unternehmen muss auch Regeln zum Umgang mit ihren Werten definieren. Oft liest man dann von «Mitarbeiter-Weisungen». Diese Regeln gelten für alle, die mit diesen Systemen arbeiten, somit auch für externe Stellen.

Folgende Punkte könnten in einer solchen Weisung enthalten sein:
- Verantwortlichkeit für Werte
- Entfernung von Werten aus dem Standort
- Rückgabe von Werten
- Untersagte Aktivitäten
- Umgang mit Datenträgern
- Datensicherung
- Virenschutz
- Nutzung von Informationssystemen
- Benutzerkonto und Passwort
- Aufgeräumte Arbeitsumgebung (Clean Desk) und Bildschirmsperren (Clear Screen)
- Internetnutzung
- E-Mail-Richtlinien
- Mobile Geräte, BYOD
- Urheberrecht
- Überwachung

Wie aufgelistet, ist auch die Rückgabe ein wichtiger Aspekt. Bereits bei den Mitarbeiter-Prozessen erwähnt (siehe Maschinenbau 1/19, ab Seite 20), sollte dies in einer Checkliste festgehalten werden. So kann sichergestellt werden, dass wirklich alle Werte wieder zurückgenommen werden.

Die Norm erwähnt explizit auch den Schutz während der Kündigungsfrist. Hier sollten Schutzmassnahmen ergriffen werden, damit nicht noch Informationen (geistiges Eigentum) entwendet werden können.

Klassifizierung

Eine weitere Anforderung ist die Klassifizierung von Informationen. In vielen Unternehmen reichen dazu drei Kategorien:

Öffentlich

Die Veröffentlichung der Information würde die Organisation auf keine Weise beeinträchtigen
- Information ist öffentlich verfügbar.

Intern

Unberechtigter Zugang zur Information könnte geringere Schäden und/oder Unannehmlichkeiten für die Organisation verursachen
- Information ist für alle Mitarbeiter und ausgesuchte Dritte verfügbar.

Vertraulich

Unberechtigter Zugang zur Information könnte katastrophalen (irreparablen) Schaden für das Geschäft und/oder das Ansehen der Organisation verursachen
- Information ist nur einzelnen Mitarbeitern zugänglich.

Selten kann es vorkommen, dass auch «geheim» noch aufgeführt wird. Für jede Kategorie gilt es im Anschluss das Schutzniveau zu definieren. Dabei gilt es, die geschäftlichen Anforderungen sowie die rechtlichen Vorgaben zu berücksichtigen. Beachtet werden sollte, dass diese Kategorie vererbt werden kann. Wenn ein Dokument als «Vertraulich» eingestuft wird, muss auch der Server, auf dem das Dokument gespeichert ist, als «Vertraulich» betrachtet werden. Daher lohnt es sich, immer von der Information auszugehen und so die Vererbung durchzuführen. Im Standard BSI 200-2 (www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html) wird dies wie folgt gehandhabt: Erfassen der Prozesse
- werden in Anwendungen genutzt
- laufen auf IT-Systemen
- stehen in Räumen
- nutzen Kommunikationsverbindungen.

Bei der Einstufung können die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit betrachtet werden. Die jeweils höchste Kategorie wird dann für die Information verwendet. Informationen können ihre Kategorie im Verlauf der Zeit auch verändern. Zum Beispiel können vertrauliche Informationen zu einem bestimmten Zeitpunkt zu internen oder gar öffentlichen Informationen werden. Als Beispiel der Geschäftsbericht. Nach der Veröffentlichung ist dieser nicht mehr besonders schützenswert, davor aber umso mehr.

Kennzeichnung

Anhand der Klassifizierung gilt es, die entsprechenden Informationen zu kennzeichnen. Dies gilt sowohl für elektronische Informationen wie auch für Geräte, Informationen auf Papier usw. Es sollte aber darauf verzichtet werden, zu viele Angaben auf dieses Etikett an den Geräten zu schreiben. Dies könnte einem möglichen Langfinger zusätzliche Indizien liefern. Alle Mitarbeitenden sind im Umgang mit der Kennzeichnung zu schulen. Bereits bei der Erstellung eines neuen Dokuments gilt es, durch den Verfasser dieses Dokument entsprechend zu kennzeichnen. Dies kann auch in Meta-Daten von Dokumenten

Dokument-Status:	Freigegeben
Vertraulichkeitsstufe:	Intern
Version:	<VERSION>
Datum der Version:	<DATUM>
Erstellt von:	<NAME>
Letzte Bearbeitung durch:	<NAME>
Freigegeben am:	<DATUM>
Freigegeben durch:	<NAME>

Beispiel eines Informationssystems.

erfolgen. Jedoch muss beachtet werden, dass diese in der Regel nicht mit ausgedruckt werden und es kann passieren, dass ein vertrauliches Papier offen herumliegt, da es nicht nach den geforderten Klassifizierungsvorschriften behandelt wurde. Meta-Daten können aber einen zusätzlichen Schutz bieten. DLP (Data Leak Prevention)-Systeme scannen diese Meta-Daten und verhindern beispielsweise den Versand per E-Mail oder den Ausdruck von vertraulichen Dokumenten. Bei Informationssystemen (siehe Bild) könnte dies beispielsweise so aussehen. Beliebt sind auch Wasserzeichen in Dokumenten.

Datenträger

Die Norm widmet ein eigenes Unterkapitel der Handhabung von Datenträgern. Damit sind Disketten (gibt es die noch?), CD/DVD/BR, USB-Sticks in jeglicher Art und Form, Memory-Karten (zum Beispiel in Foto-Apparaten), Back-up-Tapes, aber auch Festplatten gemeint.

Datenträger sind so zu löschen, dass keine Spuren mehr darauf vorhanden sind. Dies gilt es nicht nur bei der Entsorgung, sondern auch bei der Übergabe an eine neue Person (zum Beispiel wenn der Laptop, die Arbeitsstation an eine nachfolgende Person übergeben wird). Nur Löschen mit Betriebssystem-Mitteln genügt nicht, da die Betriebssysteme nicht wirklich löschen, sondern nur den Speicherplatz als Frei markieren. Die Daten können mit entsprechenden Tools oft komplett wiederhergestellt werden. Auch ein Formatieren genügt nicht immer. Gerade bei SSDs sind die Daten dann immer noch vorhanden. Inzwischen gibt es aber genügend Tools, die Daten restlos vom Datenträger entfernen. Bei SSDs kann ein spezieller TRIM-Befehl abgesetzt werden (ATA Secure Erase) und die Daten sind ebenfalls wertlos (nicht alle SSDs unterstützen dies aber!).

Die Norm verlangt auch die ordnungsgemässe Lagerung von Datenträgern. Gerade bei Back-up-Tapes ist dies essenziell wichtig, sind diese doch die Lebensversicherung des Unternehmens. Diese gilt es kühl und trocken sowie vor magnetischen Feldern geschützt aufzubewahren.

Auch die Verschlüsselung der Daten ist eine Möglichkeit, die Informationen zu schützen. Unter Windows kann Bitlocker eingesetzt werden. Auch VeraCrypt ist eine gute Möglichkeit (mehr dazu in Maschinenbau 4/2019).

Einige Datenträger haben auch ein Maximalalter. Werden die Daten länger benötigt, müssen diese genügend früh auf neue Medien transferiert werden.

Lebensdauer von Datenspeichern:

- Magnetband: 10 bis 20 Jahre
- Kassetten: 30 Jahre
- Diskette: 3 bis 10 Jahre
- CD/DVD: 5 bis 10 Jahre unbespielt, sonst 2 bis 5 Jahre
- Blu-Ray: zirka 10 Jahre
- Festplatten: 3 bis 5 Jahre
- Flash-Speicher: 10 Jahre (bei normalem Gebrauch)

USB-Sticks ermöglichen den schnellen Transport von Daten von einem Ort an einen anderen. Jedoch können auf diesem Weg auch sehr schnell Daten «entwendet» werden. Die Kontrolle mit Bordmitteln ist nur eingeschränkt möglich. Windows kann zwar per Gruppenrichtlinie die USB-Ports generell sperren. Für viele Unternehmen ist dies aber keine gangbare Möglichkeit. Verschiedene Hersteller bieten hier Tools an, die individuelle Berechtigungen ermöglichen: von Fotokameras kann nur gelesen werden (Bilder an PC), Tastaturen und Mäuse sind erlaubt usw. Müssen Daten trotzdem einmal auf einen USB-Datenträger kopiert werden, können diese protokolliert oder gar als zusätzliche Kopie an einen weiteren Ort kopiert werden (Nachvollziehbarkeit).

Das zweite Kapitel geht dann auf die Entsorgung von Datenträger ein. Gerade auf Festplatten sind viele Daten vorhanden. Wahlweise werden diese sicher gelöscht und erst dann (dies ist aber mit Aufwand verbunden) oder durch ein spezialisiertes Unternehmen entsorgt. Die DIN-Norm 66399 definiert, wie Datenträger entsprechend ihrem Schutzbedarf zu entsorgen sind (https://din66399.de/). Gerade bei defekten Datenträgern ist dies die einzige sichere Möglichkeit. Verlangen Sie von Ihrem Dienstleister immer ein Vernichtungsprotokoll als Nachweis. Hinweis: natürlich können Sie auch selbst den Datenträger mechanisch zerstören. Die Verletzungsgefahr ist aber nicht unerheblich.

Definieren Sie auch, wie Sie mit defekten Datenträgern in Laptops und Arbeitsplatzgeräten umgehen. Oft wird ein Gerät zur Reparatur eingeschickt. Dann sind auch die Daten darauf nicht mehr unter Kontrolle. Eine Möglichkeit ist es, ein neues Gerät mit der kleinstmöglichen Festplatte zu bestellen, diese umgehend auszubauen und durch eine andere zu ersetzen. Bei einem Reparaturfall wird dann die Originalfestplatte wieder eingebaut. Leider funktioniert dies bei fest verlöteten Festplatten (zum Beispiel in Tablets oder Handys nicht mehr). Ein wichtiger Punkt, der gerne vergessen geht, ist auch die Festplatte in Druckern. Auch diese gilt es vor Entsorgung/Reparatur sicher zu löschen.

Der letzte Punkt in diesem Kapitel definiert Anforderungen an den Transport von Datenträgern. Auch hier gilt es Regeln zu definieren. Werden Datenträger per Kurier übermittelt, gilt es diesen im Vorfeld genau zu prüfen. Der Datenträger sollte zudem so verpackt werden, dass er vor physischer Beschädigung (Hitze, Feuchtigkeit, Magnetfelder) geschützt ist. Beim Versand sollte weiter ein Protokoll geführt werden. Als Möglichkeit könnte Einschreiben mit Rückschein genutzt werden. Besser ist es natürlich, wenn der Datenträger so verschlüsselt ist, dass wenn er abhanden kommt, niemand etwas damit anfangen kann.

Zusammenfassung

Das Normenkapitel A.8 umfasst das Erfassen von Werten (Assets), Anforderungen an die Verantwortlichen, den korrekten Umgang, Klassifizierungsvorschriften sowie den Umgang mit Datenträgern. Damit sind Werte von ihrer Entstehung bis zur Vernichtung gemäss ihren Schutzanforderungen korrekt behandelt.