Nachhaltige Datenlöschung

Gelöscht ist nicht gelöscht!

Aus Sicht des Datenschutzes ist es unerlässlich, sichere Datenlöschverfahren einzusetzen – sowohl für Festplatten als auch für mobile Datenträger. Nicht immer ist es aber wirtschaftlich, diese gleich physikalisch zu zerstören. Wir zeigen Ihnen, was Sie bei der Wiederverwendung beachten müssen und was es mit der neuen DIN 66399 auf sich hat.

Die neue DIN 66399 regelt nur die Vernichtung von Datenträgern, nicht hingegen Löschverfahren, bei denen der Datenträger anschließend weiter verwendbar ist. Nicht immer ist der Shredder aber die passende Lösung. Gerade bei hohen Festplattenpreisen lassen sich beim Weiterverkauf gebrauchter Speichermedien Kosten sparen. Vielen ist zudem nachhaltiges Handeln wichtig.

Es spricht also einiges dafür, Datenspeicher nicht zu vernichten, sondern nur die Daten darauf zu löschen.

Gefahr: Daten könnten sich rekonstruieren lassen

Gelöscht ist aber leider nicht immer gelöscht. Daten lassen sich rekonstruieren, selbst wenn die Platte formatiert, überschrieben oder grob zerkleinert wurde. Dies kann eine Gefahr für das Unternehmen darstellen, etwa wenn noch auslesbare Festplatten mit sensiblen Daten weiterverkauft werden. Es drohen erhebliche Sanktionen bis hin zu Imageschäden, wenn man eine Datenpanne offenlegen muss.

Klassifizieren Sie die Daten

Bevor Sie über die richtige Löschtechnik im Einzelfall entscheiden können, müssen Sie zunächst die Daten und die Art der Datenträger einer Inventur unterziehen. Handelt es sich um

- belanglose Daten,
- personenbezogene Daten,
- sehr sensible Daten oder gar
- Daten, die einer Schweigepflicht unterliegen?

Löschen im Sinne des BDSG

Das Bundesdatenschutzgesetz (BDSG) versteht unter „Löschen“ in § 3 Abs. 4 Nr. 5 das Unkenntlichmachen gespeicherter personenbezogener Daten. Sie werden dann als unkenntlich angenommen, wenn sich die Informationen nicht länger aus den ursprünglich gespeicherten Daten gewinnen lassen und eine weitere Verarbeitung nicht mehr möglich ist. Konkreter wird das BDSG nicht. Es finden sich aber in § 9 BDSG samt Anlage und in einigen DIN-Normen Anhaltspunkte.

Die Wiederherstellung der Daten muss unattraktiv bis unmöglich sein

Datenschützer empfehlen daher, die Stärke der Löschmaßnahmen so zu wählen, dass eine Wiederherstellung der Daten mit vertretbaren finanziellen oder materiellen Mitteln nicht nur erschwert oder unattraktiv, sondern auch praktisch nicht mehr durchführbar wäre.

Chefsache: Sicherheitsrichtlinien schaffen Klarheit

Was mit Datenträgern geschieht, die das Haus verlassen, ist eine der wichtigsten Fragen der IT-Sicherheit und sollte Chefsache sein. Die möglichen Konstellationen sind in einer Sicherheitsrichtlinie (Security Policy) zu erfassen, die auch Schutzziele und allgemeine Sicherheitsmaßnahmen als offizielle Vorgaben für das Unternehmen formuliert.

Das Unternehmens-Know-how ist zu schützen, etwa betriebsinterne Daten, Zeichnungen, Patentschriften vor der Anmeldung etc. Man sollte regeln, was geschieht, wenn Mitarbeiter von zu Hause aus arbeiten, etwa vom privaten PC aus oder auf dem privaten Smartphone.

Welches Löschverfahren ist für welche Daten geeignet?

Die Technik sollte dem Schutzbedarf der Daten, der jeweiligen Risikostufe, gerecht werden. Sie sollte also ausreichend sicher sein und gleichzeitig das Kosten-Nutzen-Verhältnis berücksichtigen. Es gilt das Schutzbedürfnis der Daten und die richtige Schutzmaßnahme im Vorfeld zu dokumentieren.

Tipp: Denken Sie dabei auch an Geräte wie Kopierer, die personenbezogene Daten auf versteckten internen Datenträgern speichern!

Physikalische Löschmethoden

Experten streiten darüber, welche Löschmethode die sicherste ist. Es gibt physikalische Maßnahmen mit einer mechanischen, thermischen oder magnetischen Behandlung des Datenträgers. Dazu zählen das Shreddern oder das Entmagnetisieren von Festplatten (sogenanntes Degaussen). Das Speichermedium lässt sich danach je nach Medium und Verfahren gegebenenfalls nicht mehr verwenden.

Sinnvoll für nicht mehr verwendbare Datenträger oder sehr sensible Daten

Diese Technologien sind sinnvoll bei defekten Festplatten mit sensiblen Daten, die ohnehin nicht mehr nutzbar wären. Gleiches gilt, wenn das Überschreiben aufgrund des Schutzbedarfs nicht ausreicht.

Handelt es sich z.B. um sehr sensible Daten wie geheime Unternehmensdaten, Personaldaten, Daten von Ärzten, Steuerberatern, Anwälten oder Sozialdaten, sollte man die Speichermedien nicht weitergeben und zusätzlich eine physikalische Löschmethode anwenden.