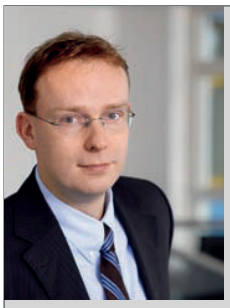


Editorial

„Dienstwagen ...,

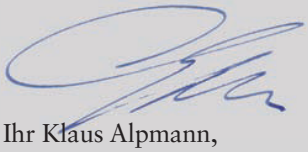
liebe Leserinnen und Leser,

lassen sich jetzt perfekt kontrollieren. Und zwar über eine neue Fahrtenbuch-Software, die laut Hersteller mit einem GPS-Ortungssystem zusammenarbeitet. Das ist ein kleines Gerät, das sich leicht in jedem Fahrzeug – auch verdeckt – installieren lässt. Ein Mobilfunk-Datenmodem überträgt dann die gesammelten Streckendaten vollautomatisch in die Fahrtenbuch-Software beim Arbeitgeber.

Der Hersteller verweist auf weitere Vorteile: „Aus den Daten lassen sich viele zusätzliche Informationen gewinnen, z.B. wie lange ein Kunde besucht wurde und ob die Besuchsberichte mit den erfassten Daten übereinstimmen, oder ob ein Fahrer vielleicht eine nicht genehmigte Sonderfahrt unternommen hat."

In der Videoüberwachung am Arbeitsplatz hat das BAG einen Eingriff in das allgemeine Persönlichkeitsrecht der Beschäftigten gesehen mit dem Argument, Arbeitnehmer dürfen nicht einem ständigen Überwachungsdruck ausgesetzt sein. Für die totale Fahrzeugüberwachung wird hoffentlich Gleiches gelten!

Mit besten Grüßen



Ihr Klaus Alpmann,
Chefredakteur Datenschutz PRAXIS

Nachhaltige Datenlöschung

Auf Nimmerwiedersehen!

Mit Software für die sanfte Tiefenreinigung bis hin zum extrem gründlichen 35-fachen Überschreiben des Datenträgers nach der Gutmann-Methode können Sie den sensibelsten Daten den Garaus machen. Methoden, die aber auch gravierende Nachteile haben: Sie kosten viel Zeit und lassen sich nur bei intakten Datenträgern anwenden. Machen Sie daher Ihrer Geschäftsleitung am besten mechanische Schredder schmackhaft. Denn sie sind die sicherste Alternative.

Nach der Begriffsbestimmung aus § 3 Abs. 4 Ziffer 5 Bundesdatenschutzgesetz (BDSG) ist Löschen „das Unkenntlichmachen gespeicherter personenbezogener Daten".

So weit ist diese Forderung verständlich – aber reicht das Unkenntlichmachen wirklich, ist Unkenntlichmachen gleich Löschen?

Die BSI-Empfehlungen zum unwiederbringlichen Löschen

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) behandelt das Thema in seinem Grundschutzhandbuch in einem eigenen Kapitel. Die empfohlenen Maßnahmen lassen sich in folgenden Handlungsleitsätzen zusammenfassen:

- Um Dateien unwiederbringlich zu löschen, müssen alle Einträge auf dem Datenträger überschrieben werden.
- Empfohlen wird eine Überschreibprozedur von mindestens zwei, besser aber drei Wiederholungen.
- Magnetische Datenträger (Disketten, Tapes, Flash-Speicher) können mit einem Löschgerät gelöscht werden. Dabei werden die Datenträger einem externen magnetischen Gleich- oder Wechselfeld ausgesetzt (Durchflutungslöschung).
- Bei defekten Festplatten, USB-Speichersticks und nicht wieder beschreibbaren CDs ist ein softwaregestütztes Löschen durch Überschreiben nicht mehr möglich. Somit bleibt nur das physische Löschen bzw. die Zerstörung.

Daten werden erst beim Überschreiben gelöscht, nicht vorher

Bei einer gelöschten Datei wird lediglich der belegte Speicher auf dem Datenträger als frei markiert. Die Daten selbst sind oftmals weiterhin vorhanden. Erst wenn der Speicherplatz überschrieben wird, kann kein Programm mehr die Daten lesen.

Vorsicht Restmagnetismus

Professionelle Datenrettungsverfahren können jedoch noch immer durch aufwendiges Messen des Restmagnetismus die Daten wiederherstellen. Erst durch ein häufiges Überschreiben der Datenspuren mit verschiedenen Bitmustern soll jegliche Schlussfolgerung auf den ursprünglichen Bit-Zustand unmöglich gemacht werden.

Vier- bis 35-faches Überschreiben

Dem US-Verteidigungsministerium genügt nach dem Standard 5220.22-M ein viermaliges Überschreiben des Datenträgers. Das BSI-Geheimschutzverfahren für Verschlusssachen verlangt dagegen siebenfaches Überschreiben mit verschiedenen Bitmustern.

Das Nonplusultra dagegen ist die Peter-Gutmann-Methode, die ein 35-maliges Überschreiben vorsieht. Von Restmagnetismus der Ursprungsdaten kann danach keine Rede mehr sein.

Gravierender Nachteil Zeitfaktor

Ist die zu löschende Festplatte noch funktionstüchtig und für weitere Ein-

Richtlinien zur Datenlöschung

- BSI-Richtlinie zum Geheimschutz von Verschlusssachen beim Einsatz von IT (VSITR): sieben Durchgänge, wobei sechs Durchgänge mit Umkehr der Bitmuster arbeiten müssen
- Standard 5220.22-M des US-Verteidigungsministeriums: insgesamt vier Mal mit verschiedenen Bitmustern
- Peter-Gutmann-Methode: 35 Überschreibungsdurchgänge der verschiedensten Art (sehr zeitaufwendig)
- DSX-Methode: gilt als besonders schnell, wird jedoch nicht mehr für als vertraulich eingestufte Daten empfohlen
- DIN 33858: Löschung magnetischer Datenträger
- DIN 32757: Vernichtung nicht magnetischer Datenträger
- BSI-Liste TL-03400: empfohlene Löschgeräte des BSI

sätze vorzubereiten, hilft meist nur ein Software-Eraser mit oben aufgeführten Überschreibungsmethoden.

Der gravierendste Nachteil ist jedoch der Zeitaufwand. 100 GB und mehr nach der Gutmann-Methode mit 35 Schreibzyklen zu eliminieren, nimmt einige Stunden in Anspruch.

Löschgeräte nach DIN 33858

Flexible magnetische Datenträger wie Disketten, Bandkassetten oder auch Videotapes lassen sich alternativ mit einem speziellen Löschgerät von verräterischen Daten befreien.

Bei diesem Verfahren wird der Datenträger einem starken Magnetfeld ausgesetzt. Die DIN 33858 sieht dafür verschiedene Anforderungsstufen vor:

- Anforderungsstufe A/Löschdämpfung mind. 45 dB: Eine Reproduktion der gespeicherten Daten ist bei erheblichem Aufwand nicht auszuschließen. Je nach Art der Datenträger sind unterschiedlich hohe Feldstärken zwischen A1 bis A3 vorgesehen.
- Anforderungsstufe B/Löschdämpfung mind. 90 dB: Eine Reproduktion ist nach dem Stand der Technik unmöglich. Auch hier sind unterschiedliche Feldstärken zwischen B1 bis B3 möglich.

Geeignete Löschgeräte, auch Degausser genannt, tragen eine Bezeichnung, aus der die erfüllten Anforderungsstufen hervorgehen, z.B. DIN 33858–A2.

Degausser eignen sich auch für defekte Festplatten

Mit einem Degausser lassen sich somit alle Arten von magnetischen Speichermedien zuverlässig löschen, auch defekte Festplatten.

Durch Entmagnetisierung mit einem Gleich- oder Wechselfeld der doppelten Feldstärke, verglichen mit der, die die Festplatte zum Schreiben benutzt, werden nicht nur die Datenspuren vernichtet, sondern auch Servo- und Wartungsinformationen gelöscht. Eine bis dahin intakte Festplatte ist nach der Behandlung im Degausser zerstört.

Die Selfmade-Methode

Bei einmalig beschreibbaren optischen Datenträgern wie CD-ROM oder WORM kann keine Löschung der Datenspuren erfolgen. Hier kommt nur eine physische Vernichtung in Frage.

Eine oft angewendete Methode ist das Zerkratzen der Datenoberfläche oder das Brechen des Mediums. Es bleibt aber die Frage, ob die Daten wirklich unwiederbringlich gelöscht sind.

Best Practice: ein Datenschredder

Analog zur DIN 32757 sind für diese Speichermedien one-4-all-Geräte erhältlich. Geeignet ist z.B. ein Multischredder, der kleinere Mengen CDs, Kreditkarten oder Papier vernichtet.

Die Restpartikel nach DIN Stufe 3 sind nicht mehr wiederherzustellen

Das Ergebnis des Schreddervorgangs sind Partikel von 4 x 30 mm – eine Wiederherstellung selbst von Papier wird als „sehr aufwendig“ bezeichnet.

Bei einer CD aus dem Abfallbehälter des Schredders dürfte eine Reproduktion selbst absoluten Spezialisten nicht mehr möglich sein.

Für Profis – ein Festplatten-Crasher

Bei Festplatten, insbesonders bei defekten Medien, gilt als sicherste Alternative der Datenlöschung die mechanische Zerstörung in kleine Fragmente. Ein Festplatten-Crasher zerlegt die mit vertraulichen Informationen gespickte Festplatte in schrottreife Kleinteile.

Eine Rekonstruktion ist auch hier so gut wie unmöglich

Wie sicher solch ein Crasher ist, zeigt die BSI-Bewertung eines Herstellers: *„Aus Sicht des BSI kann das Vernichtungsgerät Festplatten-Crasher für die Vernichtung von Festplatten schutzbedürftiger Daten, wie Firmendaten oder Daten, die dem Datenschutz gemäß BDSG unterliegen, uneingeschränkt verwendet werden.“*

Hermann Keck

Sensible Daten müssen so gut vernichtet werden, dass sie nicht rekonstruierbar sind. Das funktioniert am sichersten mit der physischen Vernichtung.