

Der digitale Papierkorb

Ordnungsgemäßes Löschen und Vernichten von Daten

Michael Gruber, IT-Security Consultant, BSP. SECURITY

In den IT-Grundschutzkatalogen gibt es mittlerweile für das Thema „Löschen und Vernichten von Daten“ einen eigenen Baustein. Was gilt es bei diesem altbekannten und noch immer vernachlässigten Thema besonders zu beachten? Und was bedeutet dies für Geschäftsprozesse der Organisation?

Die unbeabsichtigte Weitergabe von Daten durch unsachgemäßes Löschen stellt ein großes Sicherheitsrisiko für Behörden und Unternehmen dar. Passwörter, Konfigurationsdaten, kryptografische Schlüssel, vertrauliche Informationen auf Datenträgern (analog oder digital) oder in IT-Systemen können so in falsche Hände gelangen. Welche Daten sind unter Compliance Aspekten betroffen? Eine Klassifikation und Identifikation von Daten hat unter Zuhilfenahme der folgenden Aspekte zu erfolgen:

- Den ersten Hinweis liefert die Informationssicherheitsleitlinie, in der die allgemeinen Sicherheitsziele und das allgemeine Sicherheitsniveau der Organisation von der Leitungsebene postuliert werden. Daraus ist die generelle Bewertung des Schutzbedarfs „Vertraulichkeit“ abzuleiten.
- Gesetze und Rechtsvorschriften wie KontRaG, AktG, GmbHG, SGB, MaRisk, PCI DSS und UP-Bund liefern einen elementaren Rahmen für die Identifikation der Daten.
- Die interne Verarbeitungsübersicht legt aus Sicht des Bundesdatenschutzgesetzes (BDSG) entsprechende Datenquellen in der Organisation fest.
- Eine bereits durchgeführte Schutzbedarfsanalyse (BSI 100-2) oder eine eventuell vorgenommene Risikoanalyse (BSI 100-3) definiert Anwendungen und

damit verbundene IT-Systeme sowie deren Datenträger mit hohem beziehungsweise sehr hohem Schutzbedarf „Vertraulichkeit“.

Diese Betrachtung führt zu einer Landkarte der schützenswerten Daten der Organisation. Die entsprechenden Datenträger und IT-Systeme sind in noch festzulegenden Prozessen mit geeigneten technischen Verfahren ordnungsgemäß zu löschen oder zu vernichten. Unterbleibt dies, besteht die Gefahr gegen Compliance Verpflichtungen zu verstoßen.

Alternativ dazu besteht die Möglichkeit, prinzipiell und ausnahmslos alle Daten, nachdem diese nicht weiter benötigt werden, einer sicheren Entsorgung zuzuführen. Positiv an dieser Ausrichtung ist die ganzheitliche Löschung und Vernichtung von Daten. Eine eventuell unsachgemäße Entsorgung von Daten, die fälschlicherweise als nicht vertraulich identifiziert wurden, ist somit nahezu ausgeschlossen. Erkauft wird dies mit entsprechenden Mehrkosten, etwa in der Form, dass prinzipiell Festplatten, auch bei Leasinggeräten, nicht wiederverwendet, sondern vernichtet werden.

Ausgehend von der Phase der Identifikation schutzbedürftiger Daten müssen relevante Geschäftsprozesse dem sicheren Entsorgungskonzept angepasst werden. Mit anderen Worten: Den Lebenszyklus von Datenträgern und IT-Systemen

begleitend, sind von der Konzeption und Anschaffung, dem Betrieb bis hin zur Aussonderung verbindliche Maßnahmen in einer Sicherheitsrichtlinie festzulegen. Die Wirksamkeit der Maßnahmen muss im PDCA-Zyklus (Plan, Do, Check, Act) im Rahmen der Revision kontinuierlich überprüft und bei Bedarf angepasst werden.

Sondergeräte nicht vergessen

Die weitverbreiteten Multifunktionsdrucker sind in der Regel mit Festplatten ausgerüstet, auf denen beim Kopieren, Scannen oder Drucken die zu verarbeitenden Dokumente (zwischen-)gespeichert werden. Im Rahmen der Erstellung der Sicherheitsrichtlinie ist zu klären, ob diese Daten automatisch sicher gelöscht werden und welches Lösungsverfahren zum Einsatz kommt. Kann bei der Reparatur des Multifunktionsdruckers (Gerätetausch) die Festplatte in unbefugte Hände gelangen? Bei der Untersuchung von Festplatten aus Multifunktionsdruckern konnte BSP. SECURITY einen großen Teil der einstmals verarbeiteten Daten rekonstruieren. Dazu wurden nur Open-Source Forensik-Tools wie „foremost“ verwendet.

Die Weitergabe von ausgemusterter Hardware an Mitarbeiter oder an andere Interessenten geschieht im Regelfall nach „Löschen“ der Festplatte mit dem Format-Kommando

des Betriebssystems. Oft wird auf eine weitere Behandlung mit speziellen Löschr-Programmen verzichtet, entweder, weil die Notwendigkeit nicht erkannt wird oder die Zeit fehlt. Die ursprünglichen Daten befinden sich daher immer noch auf dem Datenträger und könnten sehr einfach wieder hergestellt werden. Zudem besteht die Gefahr, dass sich durch die Architektur von Dateisystemen sogenannter File-Slack auf der Festplatte befindet. Damit werden zufällige Daten aus dem Arbeitsspeicher bezeichnet, die das Betriebssystem für das Auffüllen nicht komplett belegter Cluster verwendet. Besteht eine Datei aus nur einem ASCII-Zeichen und belegt damit ein Byte auf der Festplatte, so werden bei NTFS 4095 Bytes als File-Slack verwendet um den Cluster komplett auszufüllen. Die Fülldaten aus dem Arbeitsspeicher können alle möglichen Informationen enthalten, darunter E-Mail-Fragmente, Textstücke, Passwörter und kryptografische Schlüssel. Auch nach dem Löschen der Dateien und der Formatierung mit Mitteln des Betriebssystems bleiben diese Daten lesbar.

Sicherheitsrichtlinie gut vorbereiten

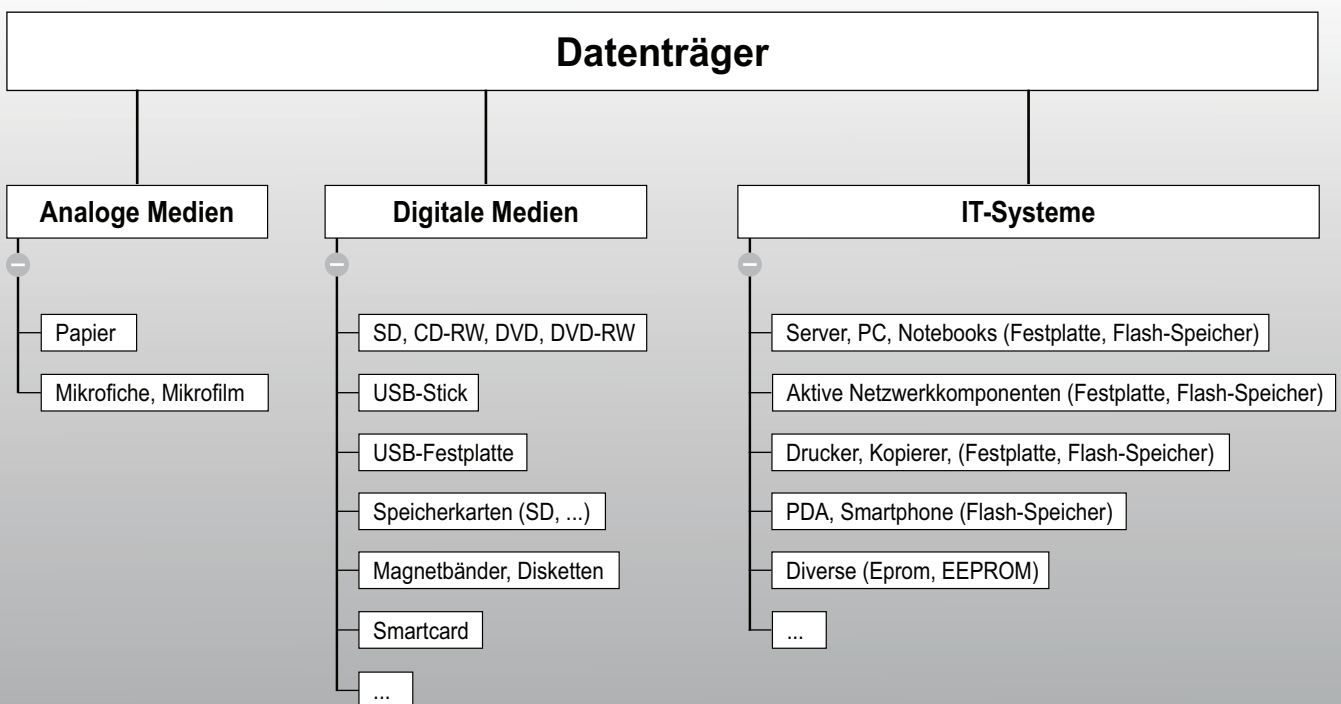
Angesichts der Fülle verschiedenster Datenträger und IT-Systeme kann die zu erstellende Sicherheitsrichtlinie sehr umfangreich und komplex werden. Die Strategie muss sich am Sicherheitsniveau der Organisation orientieren und den technischen Spezifikationen von Datenträgern und IT-Systemen entsprechen. Bei der Klärung der technischen Fragen zur sicheren Datenentsorgung bestimmen die angeführten Compliance Gesichtspunkte den Rahmen. Welche Methode im Einzelnen zum Einsatz kommen soll, hängt stark vom entsprechenden Medium beziehungsweise IT-System ab:

- Können Daten überhaupt gelöscht werden? Bei Papier und nur einmal beschreibbaren digitalen Datenträgern stellt sich diese Frage nicht – hier kommt prinzipiell nur die Vernichtung infrage.
- Mit welchen Verfahren können Daten zuverlässig gelöscht werden? Kann durch einmaliges

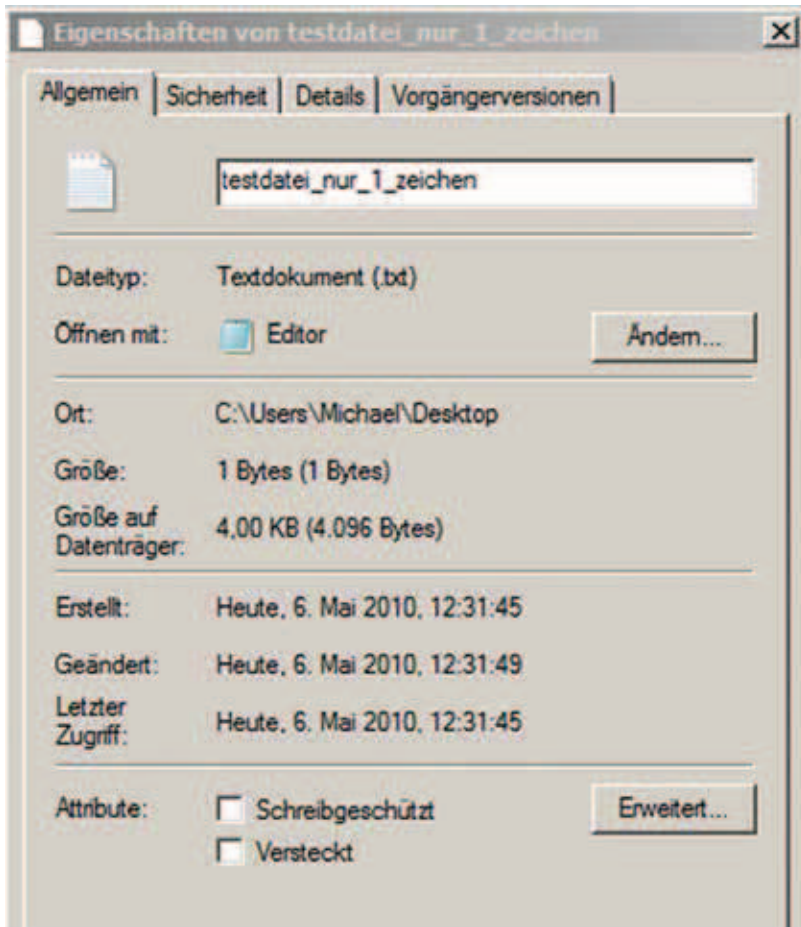
oder mehrmaliges Überschreiben mit zufälligen Bitmustern eine Rekonstruktion der Daten verhindert werden? Ist der Einsatz des UNIX-Kommandos „dd“ ausreichend, oder muss ein Tool wie „eraser“ oder das BSI-Programm „VS-Clean“ zum Einsatz kommen?

- Erfolgt die Entsorgung (Löschung und/oder Vernichtung) von Daten durch die eigene Organisation oder durch eine Spezialfirma?
- Falls eine Spezialfirma die Daten entsorgt, ist zu klären, ob dies im Hoheitsbereich der Organisation geschieht, oder ob die Daten erst zum Entsorger transportiert werden müssen, was mit einem Risiko verbunden ist.

Die BSI IT-Grundschutzkataloge liefern mit den Maßnahmen „M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten“ und „M 2.433 Überblick über Methoden zur Löschung und Vernichtung von Daten“ eine gute Übersicht (vgl. auch FOX[09]). Die



Vielfältige Quellen: Landkarte der schützenswerten Daten



Füllmaterial File-Slack: Das Betriebssystem füllt den Cluster auf der Festplatte mit Zufallsinhalten aus dem Arbeitsspeicher

sicherste, wenn auch vielleicht teuerste Lösung, ist die Vernichtung von Datenträgern und IT-Systemen. Aber auch entsprechende Lösungsverfahren werden im neuen Baustein „B 1.15 Löschen und Vernichten von Daten“ aufgezeigt und bewertet. Das ordnungsgemäße Löschen oder Vernichten von Daten muss integraler Bestandteil eines ganzheitlichen Informationssicherheits-Managementsystems (ISMS) sein. Ohne entsprechende Regelungen besteht ein hohes Risiko, dass schutzbedürftige Informationen in falsche Hände gelangen. Neben der technischen Herausforderung der korrekten Umsetzung, müssen auch die Compliance-Gesichtspunkte im Auge behalten werden. ■

[BSI 09]: BSI: IT-Grundschutzkataloge, 2009, 11. EL

[FOX 09]: Fox, Dirk: Sicheres Löschen von Daten auf Festplatten, in DuD (Datenschutz und Datensicherheit) 2/2009, S.110-113

Hier abonnieren



IT-Grundschutz
Informationsdienst

Neu seit Mai 2010:

Profitieren Sie zusätzlich von einem Abonnement:

Leser erhalten gratis die Zugangsdaten zum Heftarchiv mit Zugriffsmöglichkeit auf alle Artikel ab Ausgabe 1/2009

Der Informationsdienst „IT-Grundschutz“ ist eine ideale aktuelle Ergänzung zu den IT-Grundschutz-Katalogen. Der monatlich erscheinende Informationsdienst liefert Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen - leicht verständlich und praxisnah.

Abonnement-Bestellung an Fax +49 6725 5994

Ja, ich abonniere bis auf Widerruf den Informationsdienst „IT-Grundschutz“ ab Ausgabe _____ zum Jahresbezugpreis (10 Ausgaben, davon 2 Doppelausgaben) von 98,00 € (Inland) / 116,10 € (Ausland) inkl. MwSt. und Versandkosten (Schweiz: 187,00 SFr).

Ich kann das Abonnement jederzeit kündigen. Zuviel bezahlte Abo-Gebühren werden rückerstattet. Ich bin damit einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weiterleiten kann.

Absender / Firmenstempel _____

SecuMedia

Der Verlag für
Sicherheits-Informationen

SecuMedia Verlag
Postfach 12 34, 55205 Ingelheim
vertrieb@secumedia.de
Tel. +49 6725 9304-0

Datum Zeichen Unterschrift

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · IT-Grundschutz 2010/7

Die SecuMedia Verlags GmbH räumt mir das Recht ein, diese Bestellung innerhalb 14 Tagen ab Bestelldatum zu widerrufen.