Certus Software

Certus löscht Daten DSGVO-konform

06.06.2018

IT-Sicherheit, Nr. 3, S. 36-37



Bild: ©depositphotos.com/Erdosain

DS-GVO: In sieben Schritten zur zertifizierten, revisionssicheren Datenlöschung

# IT lernt korrekt vergessen

Im Zuge der Europäischen DS-GVO, die seit dem 25. Mai 2018 gilt, ändern sich einige Regelungen hinsichtlich des Datenschutzes. IT-Verantwortliche müssen dringender denn je wissen, wo ihre Daten liegen und ob zu löschende Daten wirklich korrekt gelöscht wurden. Das gilt auch für Dokumente und Datenbanken, die auf Festplatten und Storage-Systemen lagern, die Unternehmen ausrangieren. Diese stellen sonst eine ernst zu nehmende Bedrohung für das Unternehmen dar. Fachgerechte Entsorgung von Daten im Allgemeinen und personenbezogenen Daten im Besonderen muss daher fest ins Lebenszyklusmanagement für Informationen integriert sein.

Die Herausforderung: Viele Unternehmen haben weder einen Datenschutzbeauftragten noch feste Vorgaben für die Außerbetriebnahme von Datenträgern. Eine Studie von techconsult beziffert ihren Anteil auf 25 Prozent. In jedem fünften Unternehmen wurden der Untersuchung zufolge bereits einmal defekte, ausrangierte Festplatten gestohlen. Um dies zu vermeiden, muss der IT-Leiter unbedingt die Inhalte der Verordnung kennen und entsprechend umsetzen. Denn wer sich hier Fehler erlaubt, bringt sein Unternehmen in Schwierigkeiten: Seit Mai 2018 müssen Unternehmen, die ihre Daten nicht ordnungsgemäß halten, löschen oder ihren Verbleib lückenlos belegen können, mit Bußgeldern von bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweit erzielten Vorjahresumsatzes rechnen.

## Das Recht auf Löschung

Artikel 17 der DS-GVO spezifiziert das „Recht auf Löschung" personenbezogener Daten. Das bedeutet: Relevante Informationen müssen jederzeit auffindbar sein und zuverlässig gelöscht werden können. Der IT-Verantwortliche muss revisionssicher belegen können, dass die Daten sicher gelöscht wurden. Wer eine professionelle Datenlöschungslösung einsetzt, ist in der Regel auf der sicheren Seite. Denn Anbieter zertifizierter Datenlöschungen übernehmen die Garantie dafür, dass die Daten tatsächlich gelöscht sind und belegen dies lückenlos.

## Wer die Wahl hat, hat die Qual

IT-Administratoren können auf eine Reihe etablierter Lösungen im Markt zurückgreifen. Vom Datenlöschungs-Service bis zur Cloud-Lösung bieten Hersteller eine breite Palette an Möglichkeiten. Bei der Auswahl geeigneter Lösungen für Datenlöschungen sollte der Administrator besonders auf folgende Punkte achten:

***1. Hohe und aktuelle Zertifizierungsstandards***

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt Richtlinien für zertifizierte Datenlöschungen vor, die Hersteller von Datenlöschprodukten einhalten sollten. Es gibt jedoch nur wenige Anbieter, die den höchsten Standard erfüllen. Die erste Wahl sollten Lösungen sein, die entsprechend der Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) geprüft sind. Weltweit gibt es nur drei Unternehmen, die nicht nur einen Nachweis über die erfolgte Löschung erbringen, sondern deren gesamter Löschungsprozess zertifiziert ist.

Zusätzlich zur Zertifizierung ist es ratsam, auf das Herkunftsland des Löschungs-Anbieters zu achten. Aufgrund der in Europa geltenden und weitgehend durchgesetzten Datenschutzgesetze sind Unternehmen mit hiesigem Sitz vertrauenswürdiger als beispielsweise Hersteller aus den USA.

***2. Revisionssichere Datenlöschprotokolle***

Zertifizierte Datenlöschungen sollten automatisch ein Löschprotokoll auslösen, das sicher übertragen, gespeichert und revisionssicher vorgehalten wird. Kommt eine cloud-basierte Lösung zum Einsatz ist es außerdem wichtig, dass sich Löschprotokolle und Zertifikate sicher aus der Cloud übertragen und im Netzwerk ablegen lassen. Hier ist wichtig, dass das IT-Sicherheits-Verschlüsselungsprotokoll einen hohen Standard beim Zugriff auf die Cloud-Verwaltungsfunktion erfüllt. Als derzeit sicherster Standard gilt TLS v1.2.

Es ist ferner darauf zu achten, dass der Prozess der Datensicherheit während der Übertragung zertifiziert ist. Die Lösung muss tatsächlich für jeden Prozess zertifiziert sein,

Certus löscht Daten DSGVO-konform

06.06.2018

IT-Sicherheit, Nr. 3, S. 36-37

nicht nur die Löschung an sich oder das Unternehmen selbst.

### 3. Einfache und zentrale Verwaltung von Löschlizenzen

Die Arbeit des Datenschutzbeauftragten wird immer komplexer und empfindliche Bußgelder hängen wie ein Damoklesschwert über ihm. Er muss deshalb in der Lage sein, jeden einzelnen Schritt nachvollziehen und ohne großen Aufwand in Reportings präsentieren zu können. Eine zentrale Management-Plattform ist die beste Möglichkeit, Informationen über Löschungen revisionssicher und übersichtlich vorzuhalten. Sie spart viel Zeit und liefert in verschiedenen Formaten Reports und Audit-Hardware-Informationen. Idealerweise kann sie die Ergebnisse in die Cloud speichern. Top-Features in diesem Bereich sind:

- die Generierung einzelner Löschberichte als PDF, XML, HTML und XLS;
- ein integrierter Überprüfungsmechanismus (hexviewer) – damit lässt sich die Löschung visuell überprüfen und Ergebnisse sind sofort ersichtlich;
- ein individuell einstellbarer Upload im Management-Tool (auf dem Speichermedium, manuell oder automatisch).

Ein solches Management-Tool können auch User und Kunden verwalten. Das ermöglicht die transparente Postenzuordnung und Auftragsabwicklung. Gute Datenlöschungs-Lösungen haben außerdem die Funktion automatischer Updates.

### 4. Offline-Datenlöschungen

Unternehmen, die nicht über die Cloud löschen möchten, können sich auch für eine Lösung entscheiden, die mit den gleichen Leistungsmerkmalen ausgestattet auch im Offline-Modus funktioniert. Es gibt Hersteller, die vollautomatisierte LAN/PXE-Lösungen zur Datenlöschung anbieten. Wichtig ist, dass diese möglichst viele Löschmethoden unterstützen, um Anwendern viele Optionen zu bieten. Professionelle Lösungen unterstützen bis zu 13 Löschmethoden von Standard Overwrite über NSA 130-2 bis hin zum Gutmann-Algorithmus.

*Eine zentrale Management-Plattform ist die beste Möglichkeit, Informationen über Löschungen revisionssicher und übersichtlich vorzuhalten. (Quelle: Certus)*

Ausgebaute und erweiterte Datenträger sollten sich ebenso sicher löschen lassen. Hierfür gibt es Datenlöschmaschinen, die sowohl in der Cloud als auch offline löschen. So lassen sich beispielsweise auch in Hochsicherheitsgebäuden sicher zertifizierte Daten löschen.

### 5. Breite Formatunterstützung

Die eingesetzte Datenlöschungs-Lösung sollte möglichst viele Speichermedien unterstützen. So werden dem IT-Administrator keine unnötigen Steine in den Weg gelegt. Besonders wichtig sind zentrale Technologien wie SSD, IDE, SATA, SCSI, SAS, Fibre-Channel, USB- und RAID – die marktführenden Lösungen unterstützen alle Formate.

### 6. Individuelles Reporting

Datenschutzbeauftragte oder IT-Verantwortliche müssen für unterschiedliche Zwecke Reportings anfertigen. Entsprechend kann es sehr unterschiedliche Anforderungen an Inhalt und Format geben. Um hier einen effizienten Workflow sicherzustellen, sollte eine geeignete Datenlöschungs-Lösung unbedingt über ein anpassbares Lösch-, Audit- und Hardware-Reporting verfügen, in dem alle Hardware-Informationen individuell wählbar sind und der Anwender ganz einfach definieren kann, was in das Reporting einfließen soll. Auf diese Weise lassen sich Audit-Reports für die weitere Bearbeitung gestalten oder die Daten direkt in ein Web-Portal oder ein ERP-System importieren.

### 7. 24/7-Support

Seriöse Datenlöschungs-Anbieter stehen ihren Kunden rund um die Uhr auch für kurzfristigen Support zur Verfügung.

## Fazit

Für die Verwaltung und Löschung von Daten sollten IT-Manager auf verlässliche und zertifizierte Lösungen setzen. Die Zeiten, in denen Admins um jeden Euro Budget kämpfen mussten, sollten endlich der Vergangenheit angehören. Angesichts potenziell horrend hoher Bußgelder dürfte sich für keinen Entscheidungsträger mehr die Kosten-/Nutzen-Frage in Bezug auf die Datensicherheit und lückenlose Dokumentation stellen. ■

**RUUD DE WILDT,**
CEO des Augsburger Unternehmens Certus Software