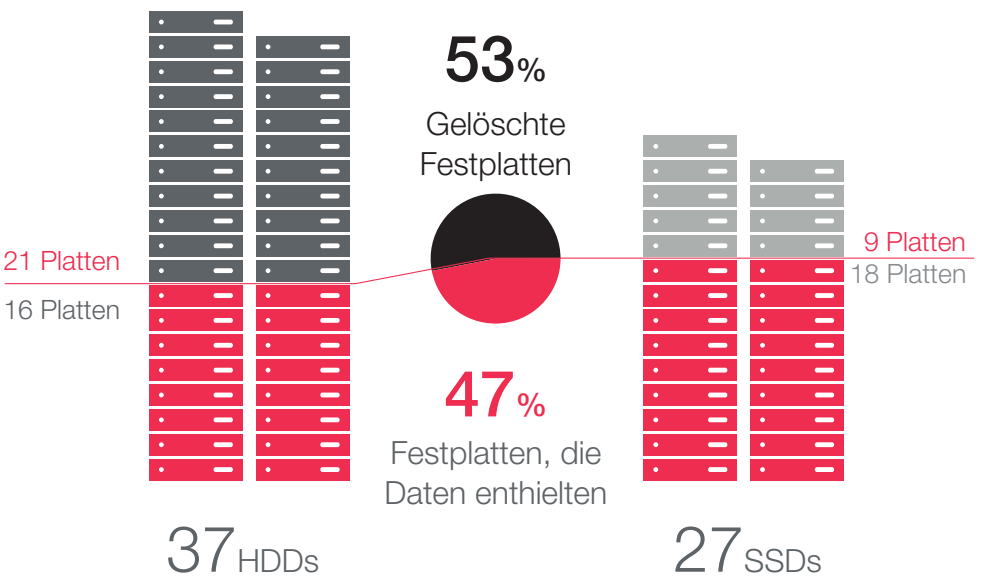
Identity for Sale

Vielfach herrscht immer noch die Meinung vor, dass das Klicken auf die Schaltfläche „Löschen“, das Leeren des Papierkorbs oder die Neuformatierung eines Laufwerks geeignete Lösungen für das schnelle und vollständige Löschen von Daten seien. Sowohl private Benutzer als auch ganze IT-Abteilungen vertrauen häufig allzu sorglos auf diese „technischen Lösungen“, um Daten von alten Geräten zu entfernen, bevor sie diese entsorgen.

Leider ist es aber nicht so, dass etwas weg ist, nur weil man es nicht mehr sehen kann. Einfaches Löschen entfernt nur das Verzeichnis zum Speicherplatz der Dateien in einem Betriebssystem, die Dateien selbst bleiben bestehen. Häufig reicht einfache Datenrettungssoftware aus, um gelöschte Informationen wiederherzustellen, von denen der vorherige Besitzer überzeugt war, sie sicher gelöscht zu haben.

Anzahl der Festplatten mitkritischen Daten

Kroll Ontrack hat eine globale Studie zum Thema Daten-sicherheit durchgeführt. Das auf Datenrettung spezialisierte Unternehmen analysierte hierzu gebrauchte Laufwerke aus den USA, Deutschland, Frankreich, Italien, dem asiatisch-pazifischen Raum, Polen und Großbritannien, um zu sehen, ob nach dem Weiterverkauf noch Datenspuren darauf zu finden waren. Auf fast der Hälfte der untersuchten Laufwerke war dies der Fall (30 von insgesamt 64 Laufwerken).



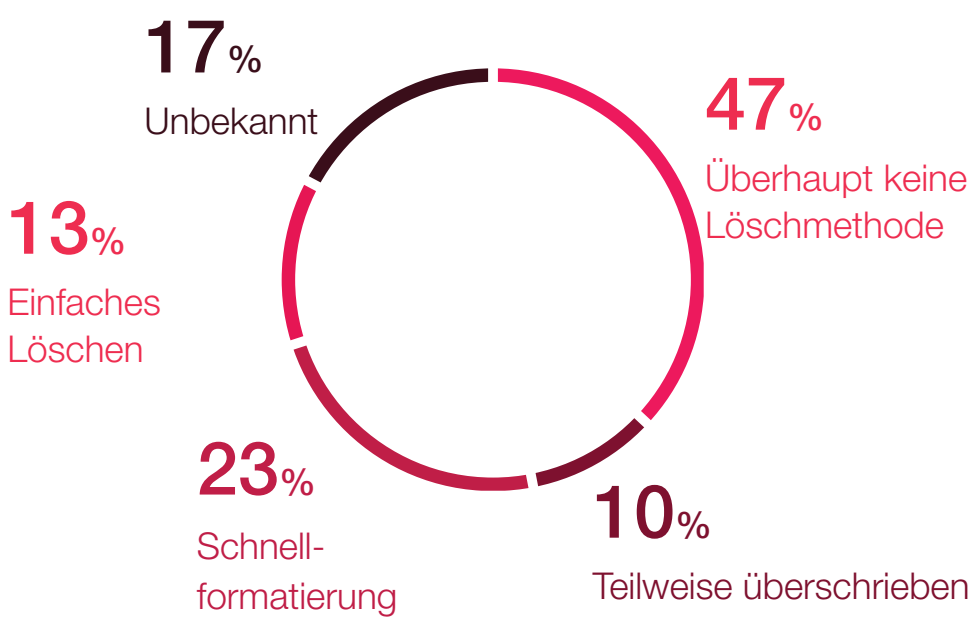
Gelöscht bedeuet nicht unbedingt “weg” - oder wie schützt man seine Identität?

Es zeigte sich, dass die Vorbesitzer mit unterschiedlichen, allerdings auch ungeeigneten Methoden versucht hatten, die enthaltenen Daten zu löschen und sich daher ein Großteil wiederherstellen ließ. Damit wird der Verkauf von persönlichen digitalen Geräten zur Frage des Identitätsschutzes.

Von den dreißig Laufwerken, aus denen Daten wiederhergestellt werden konnten, war bei elf – also erstaunlichen 37 Prozent – schon gar kein Versuch unternommen worden, die enthaltenen Daten zu löschen. Bei vier Laufwerken (13 Prozent) war nur eine einfache Löschung und bei sieben (23 Prozent) eine Schnellformatierung durchgeführt worden.

Drei Laufwerke (10 Prozent) waren teilweise überschrieben worden. Bei fünf Laufwerken (17 Prozent), bei denen Daten wiederhergestellt werden konnten, ließ sich nicht feststellen, welche Löschmethode zuvor angewendet worden war. Insgesamt waren alle Versuche ungenügend und nicht wirklich erfolgreich. Klar wurde dabei auf jeden Fall eines: Anwender setzen ihre Identität und Privatsphäre viel zu leicht aufs Spiel, indem sie unzureichende Löschmethoden verwenden, statt sich für eine sichere und dauerhafte Löschung zu entscheiden.

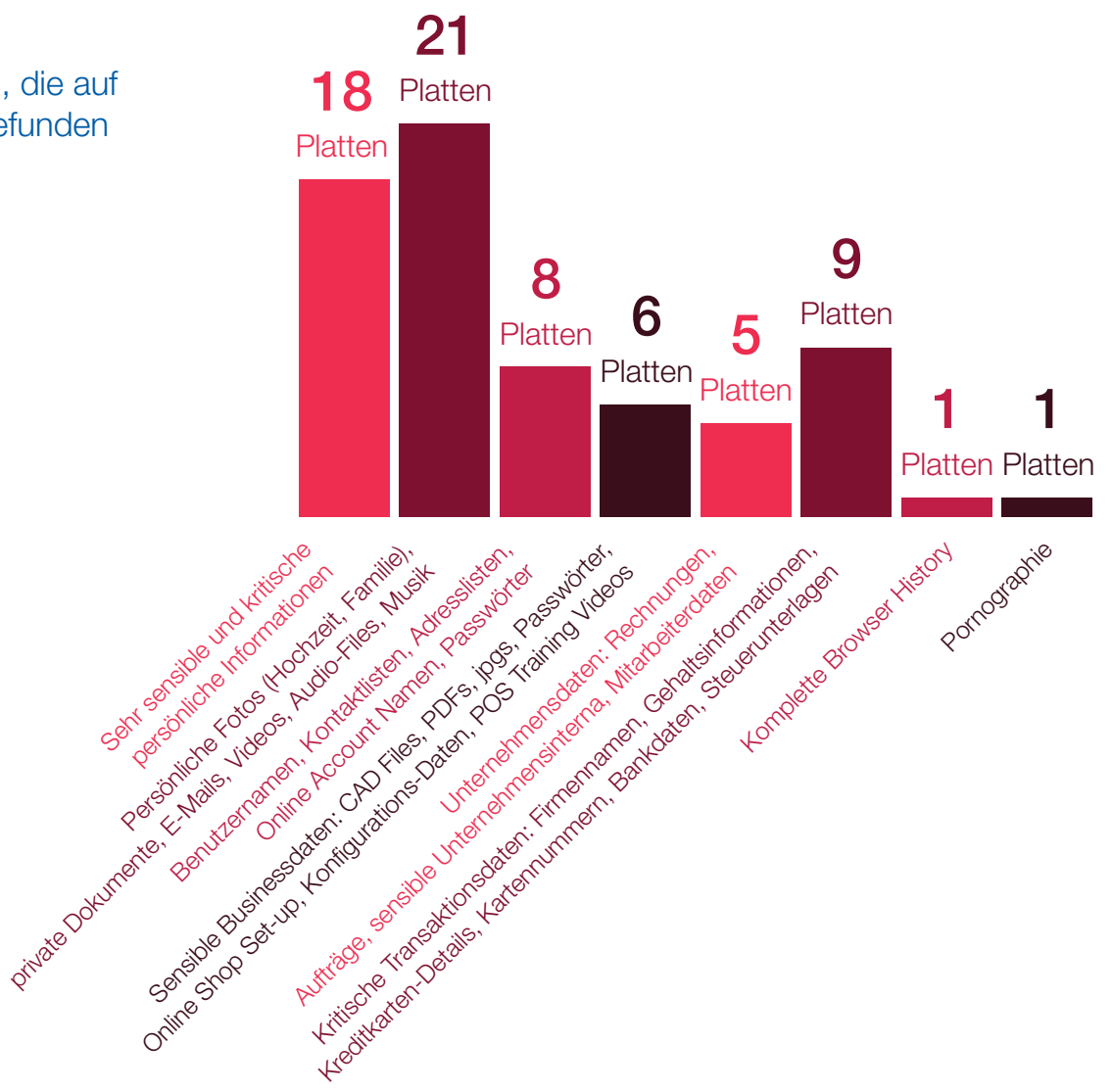
Angewendete Löschmethoden auf den Festplatten, auf welchen Daten gefunden werden konnten.



Setzen Sie Ihre Privatssphäre nicht aufs Spiel

Eines der untersuchten Laufwerke erwies sich als gutes Beispiel für die Gefahr, der sich Firmen und Einzelpersonen aussetzen, wenn Datenspuren nicht sicher gelöscht werden. Es hatte einem Unternehmen gehört, das über einen Dienstleister alte Laufwerke löschen und verkaufen ließ. Nichtsdestotrotz konnte eine Fülle von hochsensiblen Informationen herausgezogen werden, darunter Benutzernamen, Adressen, Telefonnummern und Kreditkarten-details.

Persönliche Daten, die auf den Festplatten gefunden werden konnten



Ontrack®

Richtig löschen - aber wie?

Kroll Ontrack hat ein paar Methoden definiert, die man vermeiden sollte, und einige, die das Unternehmen empfiehlt, wenn persönliche Daten sicher und dauerhaft gelöscht werden sollen.

Nicht empfohlen: Schnellformatierung

Mit dieser Methode wird nur der Metadatenbereich des Laufwerks neu erstellt, um zusätzlichen Speicher freizugeben. Die Daten selbst werden jedoch nicht gelöscht. Eine vollständige Neuformatierung wird ebenfalls nicht empfohlen. Hierbei werden lediglich alle Sektoren des Laufwerks gescannt, einschließlich der fehlerhaften Sektoren, neu geordnet und alle aktiven Daten entfernt. Die Ergebnisse hängen dabei vom Betriebssystem ab und können variieren.

Low-level Formatierung: effektiv aber zeitaufwändig

Bei einer Low-Level-Formatierung wird das Laufwerk auf unterster Ebene in Sektoren aufgeteilt und effektiv wieder auf die Werkseinstellungen zurückgesetzt. Diese Methode ist zeitaufwendig und wird daher selten verwendet – aber sie ist effektiv. Das Löschen von Daten durch das Überschreiben mit spezieller Software kann die Daten eines Geräts vollständig durch zufällige Sequenzen mit Binärziffern (Nullen und Einsen) ersetzen. Mehrfache Überschreibungen bieten zusätzliche Sicherheit, vor allem, wenn die Datenlöschung spezifische gesetzliche Überschreibungsstandards erfüllen muss.

Professionelle Lösch-Software

Mit der richtigen Softwarelösung kann ein rechtlich einwandfreies, einfach zu bedienendes und kostengünstiges Verfahren zum Löschen der Daten einzelner Geräte implementiert werden. Professionelle Produkte zeichnen sich durch mehrere Merkmale aus: unabhängige Zertifizierungen, den Einsatz internationaler Standardalgorithmen, detaillierte Berichterstattung und die Rückverfolgbarkeit der durchgeführten Löschung. Zertifizierungen sind ein besonders zuverlässiges Merkmal. Professionelle Softwarelösungen bieten in der Regel eine Löschzertifizierung an, die ein sicheres und endgültiges Säubern der Hardware garantiert. Unternehmen wie Kroll Ontrack bieten die Möglichkeit, das definitive Löschen von Daten von HDDs und SSDs zu testen und zu überprüfen – egal ob dies von einem externen Dienstanbieter oder einer Softwarelösung durchgeführt wurde.

Was ist zu beachten beim Verkauf oder Recycling von gebrauchten SSDs

Studien haben ergeben, dass Nutzer zunehmend von HDDs auf SSDs umsteigen. Ein Hauptgrund dafür sind die Vorteile, die SSDs mit sich bringen:

- Schnellere Geschwindigkeit
- Geringerer Energieverbrauch
- Robustheit dank fehlender beweglicher Teile – im Gegensatz zu HDDs

Als Experte für SSDs möchte Kingston darauf aufmerksam machen, dass sich SSDs im Hinblick auf Speicher- und Löschmechanismen gravierend von HDDs unterscheiden. Das Löschen von Daten von einem Flash-Speicher birgt technische Herausforderungen. Anders als Festplatten verfügen Flash-Speicher über einen sogenannten „Flash Translation Layer“ (FTL) für das Mapping und die Verwaltung der Inhalte auf dem Speichermedium. Wenn eine Datei geändert wird, wird die neue Version der Datei nicht am gleichen Ort gespeichert wie die alte Version, sondern an einen neuen Speicherort geschrieben. Gleichzeitig wird der FTL mit dem neuen Speicherort aktualisiert. Das heißt, dass sich noch immer Reste der ursprünglichen Datei – wenn auch nicht sichtbar – auf dem Speichermedium befinden und wiederhergestellt werden können.

SSDs dagegen verfügen über zwei Funktionen zum Löschen von Daten: Garbage Collection und TRIM. Garbage Collection entsorgt im Hintergrund Daten, die nicht länger gültig sind oder benötigt werden. Mit dem TRIM-Befehl werden Daten direkt auf dem NAND-Chip gelöscht, sodass sie nicht wiederhergestellt werden können. Es ist also möglich, dass Inhalte auf SSDs verlorengehen, und ebenso ist es möglich, diese Inhalte auf NAND-Chips wiederzufinden. Ob ein Nutzer SSDs verwendet und Daten mithilfe von TRIM oder Garbage Collection entsorgt, spielt deshalb eine wichtige Rolle, wenn es darum geht, Daten vollständig zu löschen.

All dies gilt es zu bedenken, wenn Sie SSDs in Ihrem System ersetzen oder diese recyceln. Kingston empfiehlt, dass Sie nichts dem Zufall überlassen, wenn es um das Löschen Ihrer Daten auf SSDs geht. Verlasen Sie sich auf Kroll Ontrack, um auf Nummer sicher gehen.

Maßnahmen ergreifen

Täglich werden enorme Menge an personenbezogenen Daten von Einzelpersonen und Unternehmen aller Größen gespeichert und verarbeitet. Dieser Umstand hat die deutsche Datenschutzbehörde zur Einführung angemessener Maßnahmen veranlasst, um sicherzustellen, dass diese personenbezogenen Daten vor unbefugtem Zugriff und unerlaubter Weitergabe geschützt sind. Auf europäischer Ebene ist die Einführung der neuen allgemeinen europäischen Datenschutzgrundverordnung (EU-DSGVO) Ausdruck einer Revision des Datenschutzes. Zielsetzung der neuen Regelung ist, den Schutz personenbezogener Daten an die aktuellen Herausforderungen des digitalen Zeitalters anzupassen.

Die Konsequenzen einer unsicheren Datenlöschung können sowohl für Einzelpersonen als auch für Unternehmen schwerzwiegend sein. Dabei ist das Risiko eigentlich nie auf das private Umfeld beschränkt, da in den meisten Fällen auch auf privaten Geräten arbeitsbezogene Informationen zu finden sind und somit in unerwünschte Hände fallen können. Unternehmen sind somit niemals immun gegen die Risiken des Identitätsdiebstahls und der Erpressung.

Unternehmensdaten, die in die falschen Hände geraten, können eine sehr ernste Bedrohung darstellen. Darüber hinaus setzen die Datenschutzregelungen bestimmte Entsorgungsmethoden in Übereinstimmung mit den festgelegten Aufbewahrungsfristen fest. Die gesetzlichen Regelungen der DSGVO legen dabei die Grundzüge fest, wie Unternehmen ihre Datenlöschverfahren planen sollen.

Die Vernachlässigung des Datenschutzes ist mit Sicherheit kein Kavaliersdelikt. Die gesetzlichen Regelungen sehen bei Nichtbeachtung der Bestimmungen schwere Strafmaßnahmen für Unternehmen vor. Aber auch für private Benutzer kann der betrügerische Missbrauch von personenbezogenen Daten und Erpressung weitreichende Folgen für den Einzelnen haben.

Der einfachste und effektivste Schutz gegen Datenmissbrauch ist und bleibt, Daten vor der Entsorgung oder dem Verkauf von IT-Geräten sicher und dauerhaft mit geeigneten Techniken zu löschen. Nur so kann die permanente Löschung von personenbezogenen Informationen sichergestellt werden. Nachfolgende Versuche, diese zu rekonstruieren, werden zuverlässig unterbunden und vertrauliche Informationen sind und bleiben privat.