Privacy for Sale

Eine Studie zum Datenschutz bei gebrauchten Mobilgeräten und Festplatten

blancco technology group

KrollOntrack™ By KrolLDiscovery

Einleitung

Die Faszination beim Kauf neuer elektronischer Geräte ist mittlerweile Teil unserer globalen DNA und viele Verbraucher tauschen ihre Technologien häufig aus. Eine kürzlich durchgeführte globale Studie von Kroll Ontrack und der Blancco Technology Group ergab, dass 35 % der Verbraucher aus den Deutschland, Großbritannien, USA, Kanada und Australien ihre Mobilgeräte alle zwei bis drei Jahre recyceln, verkaufen, oder verschenken und weitere 17 % sobald ein neues Gerätemodell auf dem Markt eingeführt wird.

Ein begrenztes Budget und hohe Gerätekosten können aber den Wunsch, ein neues Smartphone oder Tablet zu kaufen, maßgeblich dämpfen. Daten von IBA Research und dem Wall Street Journal zufolge stieg der durchschnittliche Neupreis eines iPhones im 4. Quartal 2014 auf 687 US-Dollar, während der eines Android-Geräts bei 254 US-Dollar liegt. Obwohl Festplatten nicht als die attraktivste elektronische Anschaffung gelten, sind sie dennoch eine Hauptkomponente der Computerarchitektur und stellen oftmals eine notwendige Investition dar. Durchschnittlich schaffen sich Nutzer alle paar Jahre eine neue Festplatte an – entweder, um die alte zu ersetzen oder sie zu erweitern.

Der Wunsch nach neuen elektronischen Geräten in Kombination mit den hohen Neuanschaffungskosten verleiten Verbraucher maßgeblich zum Verkauf und Kauf ge-brauchter Elektronik, insbesondere Computer und Mobilgeräte. Für Käufer von Second-Hand-Elektronik besteht die Motivation häufig in Kosteneinsparungen. Sie sparen dadurch hunderte Euro (oder mehr) und halten dennoch ein funktionsfähiges und brauchbares Gerät in den Händen. Unterdessen bekommen Verkäufer einen Teil oder nahezu die gesamten Kosten für das neue Gerät, welches sie sich kaufen wollen, dadurch wieder herein.

Studie auf einen Blick

- 122 gebraucht gekaufte Mobil-geräte (Smartphones) und Festplatten (HDDs, SSDs) aus Deutschland, Großbritannien und den USA
- 16 % Smartphones
- 73 % Festplatten
- 11 % Solid State Drives
- 46 % der Medien enthielten Daten

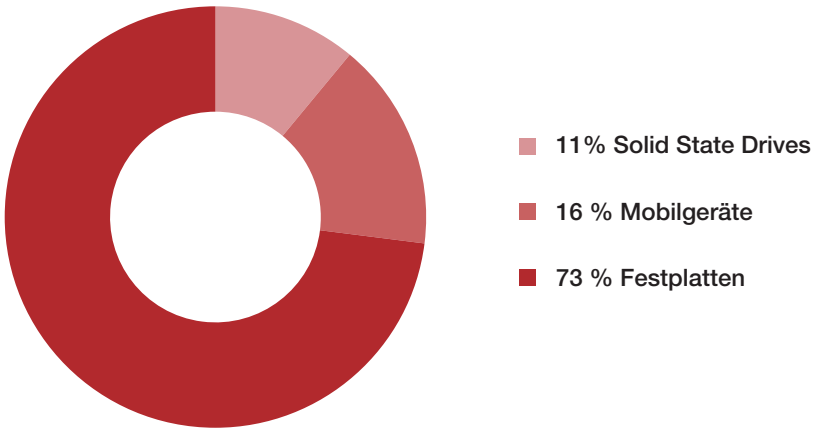
Für den Kauf oder Verkauf gebrauchter Elektronik greifen Käufer und Verkäufer oft auf Online-Marktplätze, wie eBay oder Amazon zurück. Amazon gilt mit knapp 244 Millionen aktiven Mitgliedern als einer der größten Online-Händler und zieht mit seinem Angebot und schnellen nach wie vor Käufer an. Mit seinen über 149 Millionen aktiven Käufern auf der ganzen Welt ermöglicht eBay seinen Kunden einen einfachen, schnellen und unkomplizierten Verkauf unter anderem ihrer gebrauchten Medien und IT Geräte auf der E-Commerce-Seite.

Dabei ergeben sich folgende Fragen: Welche Sicherheitsvorkehrungen treffen Verkäufer in Bezug auf ihre persönlichen Daten, wenn sie ihr Gerät auf einer dieser E-Commerce-Seiten einstellen? Treffen Verkäufer eine Art Löschmaßnahme, um ihre Daten zu schützen? Wie leicht gelangt der neue Besitzer an Restdaten auf dem Gerät? Wie können Verbraucher ihre Privatsphäre besser schützen?

Analyse und Methoden zur Datenwiederherstellung

In einem gemeinsamen Projekt entwickelten die Blancco Technology Group und Kroll Ontrack eine Datenschutzstudie, um die Auswirkungen auf die Sicherheit von – auf gebrauchten IT-Geräten gefundenen Daten – aufzuzeigen. Zwischen Mai und August 2015 kauften Mitarbeiter der Unternehmen insgesamt 122 gebrauchte Festplatten, Solid-State-Drives und Mobilgeräte von den folgenden Online-Marktplätzen in Deutschland, Großbritannien und den USA: Amazon, eBay und Gazelle.com. Sämtliche Second-Hand-Ware wurde zufällig ausgewählt und nach Verfügbarkeit erworben.

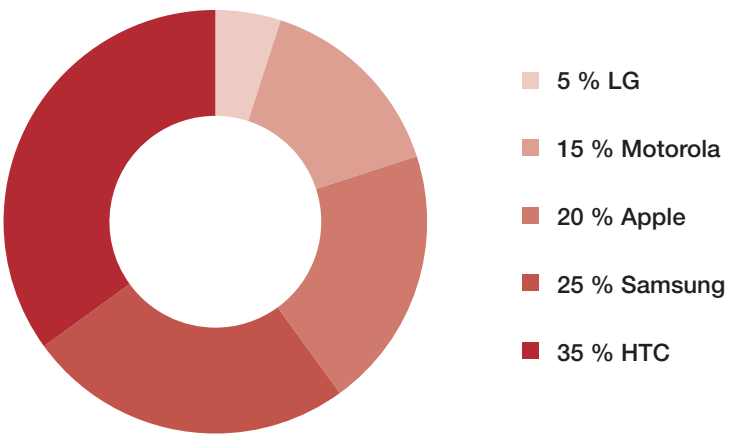
Welche Arten von elektronischen Geräten wurden in dieser Studie gekauft und analysiert?



Die Analyse und die Ergebnisse wurden in folgende Kategorien unterteilt: (1) Mobilgeräte und (2) Festplatten (HDDs)/Solid-State-Drives (SSDs). Für die Stichprobe der Mobilgeräte wurden 20 gebrauchte Mobilgeräte (darunter sowohl Geräte mit iOS- als auch Android-Betriebssystem) von fünf unterschiedlichen Herstellern gekauft. Anschließend trugen wir die gesamte wiederhergestellte Datenmenge, ihre unterschiedlichen Datentypen (d.h. E-Mails, Text-/SMS-Nachrichten, Fotos, Videos, Sofortnachrichten, identifizierter Besitzer, Gesprächsprotokolle) sowie die Datenanalyse der vom Betriebssystem wiederhergestellten Daten zusammen.

Für die Stichprobe der HDDs und SDDs kauften wir insgesamt 102 gebrauchte Laufwerke und extrahierten die wiederhergestellte Datenmenge, ermittelten die unterschiedlichen Datentypen sowie die vom ursprünglichen Besitzer durchgeführte Datenlöschmethode.

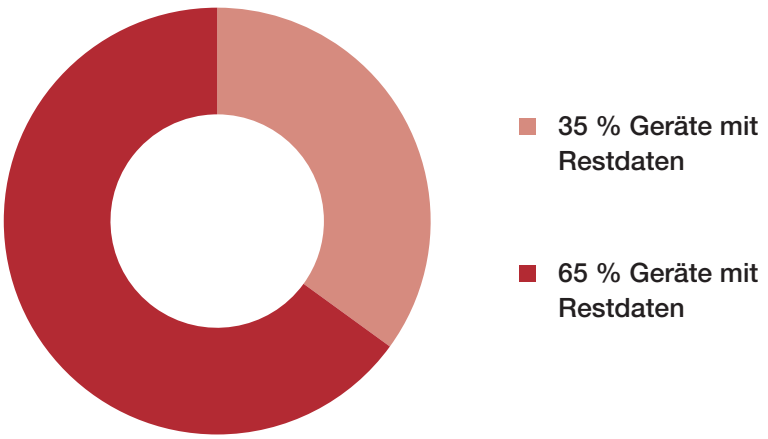
Von welchen Herstellern stammte die Stichprobe der gebrauchten Mobilgeräte, die für diese Studie analysiert wurden?



Mobilgeräte: Ergebnisse und Auswertung

Während der Untersuchung der 20 gebrauchten Mobilgeräte (20 % iOS-Geräte und 80 % Android-Geräte) fand unser Team Restdaten unterschiedlicher Typen und Mengen auf 35 % aller gekauften Geräte. Interessanterweise wurden auf den iOS-Geräten, die in dieser Studie analysiert wurden, keine Restdaten gefunden. Stattdessen konnten diese auf einigen Android-Geräten ermittelt werden, wodurch die Befürchtung entsteht, dass Personen mit dem Verkauf ihres Geräts unwissentlich auch ihre Privatsphäre verkaufen.

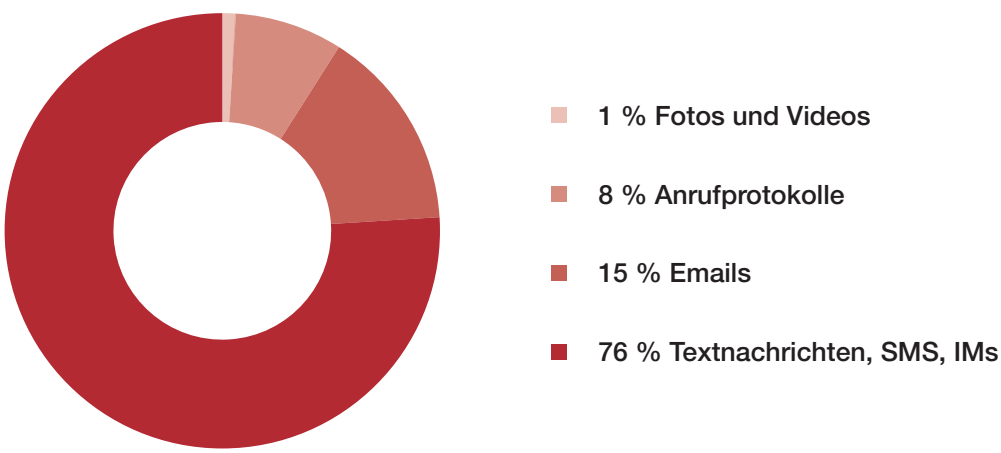
Wieviel Prozent der gebrauchten Mobilgeräte wiesen Restdaten auf?



Verbleibende E-Mails, Text-und Sofort-nachrichten können Nutzern und ihren Arbeitgebern finanzielle sowie Personen- und Rufschäden zufügen.

Weitergehende Analysen der in den gebrauchten Mobilgeräten verbleibenden Restdatentypen führten zu einigen interessanten Erkenntnissen. Angesichts der Menge an zurückgelassenen Datentypen liegt der Verdacht nahe, dass Verkäufer die Datenschutz- und Sicherheitsproblematik im Zusammenhang mit ihren E-Mails, Text- und Sofortnachrichten tatsächlich unterschätzen.

Welche Datentypen konnten auf gebrauchten Mobilgeräten wiederhergestellt werden?



Insgesamt konnten 2.153 E-Mails und 10.838 Text-/SMS-/Sofortnachrichten von den analysierten Geräten wiederhergestellt werden, was sowohl für Mobilnutzer wie auch für Unternehmen Grund zur Sorge ist. Mobilgerätebesitzer verwenden ihre Geräte zu allen möglichen Zwecken – Banking, Terminplanung, Shopping, um Essen zu bestellen, für Foto- und Videoaufnahmen und sogar für berufliche Aktivitäten. Laut einer aktuellen Studie von Tech Pro Research haben 74 % der Unternehmen bereits die Bring-Your-Own-Device-Politik (BYOD) eingeführt bzw. planen sie einzuführen, um Best-Practice-Richtlinien im Rahmen der Nutzung privater Geräte für berufliche Zwecke zu gewährleisten. Da immer mehr Unternehmen BYOD am Arbeitsplatz zulassen, ist es für Unternehmen wichtig zu verstehen, dass private Geräte Türen für Sicherheitsrisiken öffnen, vor allem wenn Mitarbeiter das Unternehmen verlassen oder ihnen gekündigt wird. Infolgedessen können vertrauliche Unternehmensdaten offengelegt, Informationen zu neuen Produkten unwissentlich übermittelt werden und vertrauliche Umsatz- und Kursinformationen in falsche Hände gelangen.

Verkäufer gebrauchter Smartphones können von alten Fotos und Videos heimgesucht werden.

Auf einem Prozent aller analysierten Mobilgeräte befanden sich noch Fotos und Videos. Dies könnte auf die falsche Annahme zurückzuführen sein, dass durch das Löschen einer Datei, diese tatsächlich verschwindet. In Wirklichkeit wird durch Drücken der „Löschen"-Taste bei gespeicherten Fotos oder Videos jedoch nicht garantiert, dass diese sicher vom Gerät entfernt werden.

Die möglicherweise aus verbleibenden Fotos und Videos gesammelten Informationen können Gefahren bergen, vor allem wenn sie in falsche Hände gelangen. Fotos können sehr genaue Lokalisierungsdaten über ihren Aufnahmeort enthalten. Demzufolge können nicht nur die Fotos selber, sondern auch die Lokalisierungsdaten öffentlich zugänglich gemacht werden, womit die Privatsphäre über den Aufenthaltsort und die Aktionen des Nutzers nicht länger gewahrt wäre. Außerdem könnten raffinierte Cyber-Kriminelle mithilfe von Werkzeugen, wie Photoshop, das Gesicht des Verkäufers in andere Bilder oder Websites unseriöser oder unangemessener Natur hineinkopieren.

So erklärt Paul Henry, IT Security Consultant für die Blancco Technology Group: „Egal, ob Sie eine Einzelperson, ein Unternehmen oder eine staatliche Einrichtung sind – mangelnde Datenlöschung kann schwerwiegende Folgen haben. Eine Haupterkenntnis unserer Studie ist, dass die meisten Menschen in irgendeiner Weise versuchet haben, ihre Daten von den elektronischen Geräten zu löschen. Gängige Löschmethoden sind bekannt und scheinen zuverlässig, beseitigen die Daten aber oft nicht dauerhaft und entsprechen nicht regulatorischen Standards. Ein aktuelles Beispiel für diese Gefahr sind Ergebnisse einer staatlichen Prüfung, die feststellte, dass zwölf US Landesbehörden, die für Besteuerung, Fahrerlaubnisse und Programme für Menschen mit psychischen Erkrankungen verantwortlich sind, inadäquate Methoden zur Vernichtung von Informationen einsetzten. Die wichtigste Lektion für Unternehmen wie Verbraucher ist es zu verstehen, welche Löschmethoden wirksam sind und regulatorische Standards erfüllen, und vor allem nicht blind zu vertrauen, dass einfaches „Löschen" Daten für immer entfernt."

Daten können nur schwer gelöscht werden und nach dem Wiederverkauf des Mobilgeräts leicht wieder sichtbar werden.

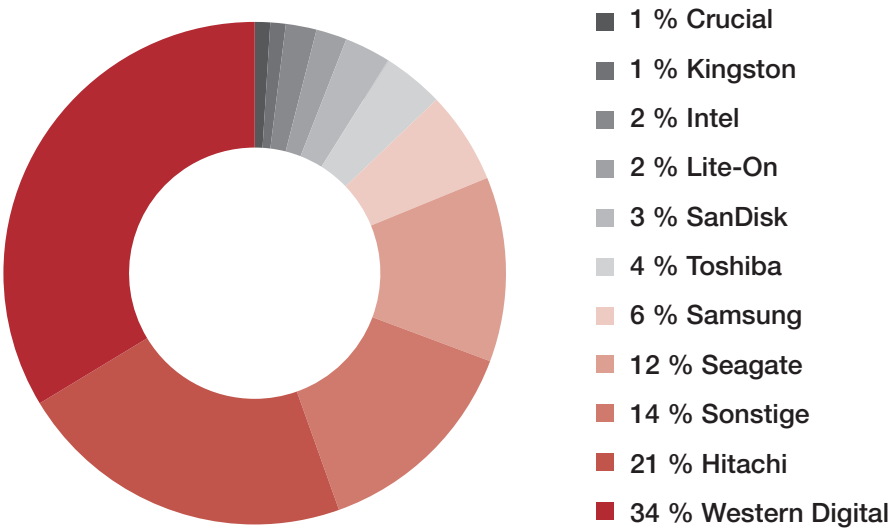
Über ein Drittel (35 %) der gekauften Second-Hand-Mobilgeräte verfügte noch über intakte Daten. Noch beunruhigender ist jedoch, dass bei über 57 % der Geräte mit Restdaten ein Löschversuch unternommen worden war. Zwei dieser Geräte enthielten noch 179 Textnachrichten, 252 Sofortnachrichten, über 75 Fotos und zwei SMS-Nachrichten. Auf Grundlage dieser Daten konnte die Identität des ursprünglichen Gerätebesitzers ermittelt werden!

Daran zeigt sich, dass nicht alle Löschmethoden effektiv alle mobilen Daten löschen. Viele gern genutzte Methoden hinterlassen eine bedeutende Menge an Daten auf dem Mobiltelefon. Außerdem können durch eine unvollständige Löschung ebenfalls Daten zurückbleiben. Bei Android-Geräten können unwirksame Löschungen deshalb auftreten, weil die Nutzer die Zurücksetzung auf die Werkeinstellung zur vollständigen Entfernung ihrer Daten als ausreichend erachteten. Im Endeffekt hinterlassen im Fall der genannten Beispiele die als „gelöscht" eingestuften Informationen (u. a. auf externen SD- oder SIM-Karten) noch intakte Daten auf dem Gerät.

Tatsächlich werden durch das manuelle Löschen von Daten oder das einfache Abmelden von einer App die Daten nicht vom Gerät entfernt. Das Löschen der Daten unterbindet nur die Fähigkeit des Mobilgeräts, die Daten wiederzufinden. Die Daten bleiben bestehen und können wiederhergestellt werden. Um die Daten unwiderruflich zu löschen, müssen sie überschrieben werden. Die Zurücksetzung auf die Werkeinstellungen, eine Methode, die großes Vertrauen genießt, erwies sich in einigen Fällen als wirksam, in anderen allerdings weniger. Jedes Betriebssystem ist anders und Löschmethoden, die für iOS funktionieren, könnten für Android-Geräte ungeeignet sein. Diese Methoden sind nicht nur von dem spezifischen Betriebssystem abhängig, sondern können auch je nach Gerätehersteller oder Gerätemodell desselben Herstellers variieren. Wenn die Zurücksetzung auf die Werkeinstellungen nicht hundertprozentig erfolgreich war, ist es ein Leichtes, mithilfe einer einfachen Google-Suche Software zu finden, die die Daten schnell wiederherstellen kann.

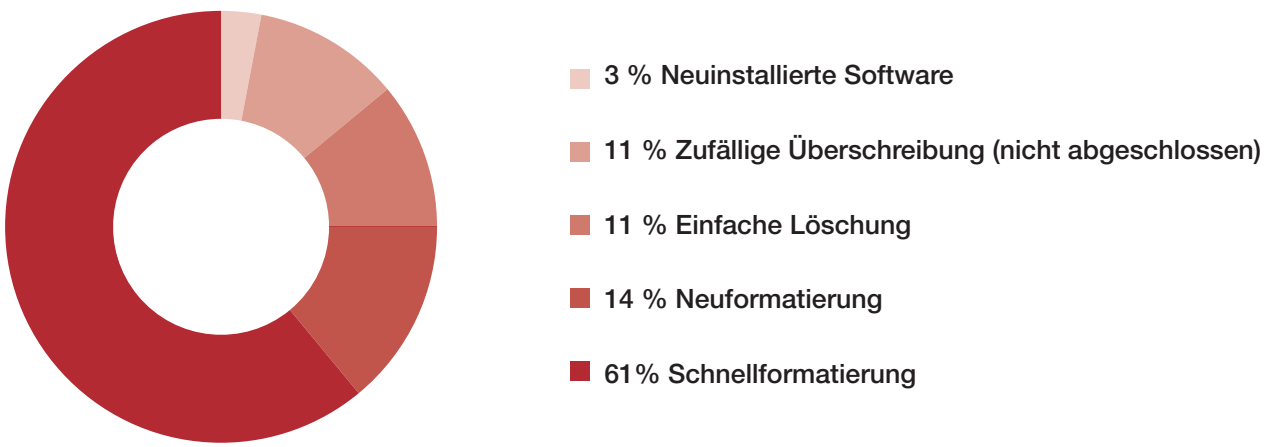
Festplatten: Ergebnisse & Diskussion

Von welchen Herstellern stammen die Festplatten und SSDs, die in dieser Studie untersucht wurden?



Aus der Analyse der Festplatten und Solid-State-Drives von 10 unterschiedlichen Herstellern ergab sich, dass nahezu die Hälfte (48 %) noch Daten aufwiesen, die für die ursprünglichen Besitzer ein Sicherheitsrisiko darstellen könnten.

Welche Methode wurde angewendet, um die Daten von den Laufwerken zu löschen?



Die einfache Datenlöschung löst bei Festplattennutzern fälschlicherweise ein Gefühl der Sicherheit aus.

Bei 75 % der Festplatten und Solid State Drives mit Restdaten wurde zuvor ein Löschversuch durchgeführt. Nur 25 % wurden ohne vorgenommene Löschmethode weiterverkauft. Dies zeigt, dass Verkäufer um die dauerhafte Löschung der Daten bemüht sind, sie aber keine rundum wirksame Lösung verwenden. Auf vier der Laufwerke (11 %) wurde lediglich eine einfache Löschung durchgeführt. Der Nutzer hat also die Datei einfach gelöscht oder in den Papierkorb verschoben. Bei dieser Löschmethode konnten problemlos 100 % der gespeicherten Daten wiederhergestellt werden. Genauer gesagt wurden auf diesen vier Laufwerken insgesamt 444.000 Dateien gefunden.

Wenn Sie Dateien einfach von Ihrer HDD oder SSD löschen, bleiben die Dateidaten auf dem Laufwerk. In Wirklichkeit löschen Sie nur den Verweis auf die Datei. Stellen Sie sich Ihr Laufwerk wie eine Bibliothek vor. Um das gewünschte Buch zu finden, erhalten Sie eine Referenznummer aus der Datenbank der Bibliothek – und die führt sie zu dem Abschnitt in der Bibliothek, in dem das Buch physisch aufzufinden ist. Stellen Sie sich vor, das Buch wurde aus der Datenbank der Bibliothek entfernt und es existieren keine Verweise mehr auf seinen Aufenthaltsort. Das Buch bleibt weiterhin in der Bibliothek, jedoch bedarf es jetzt anspruchsvollerer Methoden, um es wieder ausfindig zu machen. Das gleiche Prinzip lässt sich auf die Löschung von Dateien anwenden.

Die „Schnellformatierung" und Neuformatierung sind die Standardmethoden, die Verbraucher zur Löschung ihrer persönlichen Informationen von alten Festplatten anwenden.

Wenn Laufwerke am Ende ihrer Lebensdauer angekommen sind und ein Austausch unvermeidbar ist, nutzen viele zur Gewährleistung des Datenschutzes die einfachsten Methoden für die Datenlöschung. Unsere Studie über 102 gebrauchte HDDs und SSDs bestätigte die Beliebtheit dieser Standardmethode erneut und ergab, dass bei 61 % der Laufwerke, bei welchen eine „Schnellformatierung" durchgeführt wurde, noch Daten vorhanden waren.

Dies kann ein ernsthaftes Problem darstellen, zumal auf 81 % aller schnellformatierten Laufwerke noch Daten vorhanden waren. Dies entspricht einer aktuellen von BT und SIMS Recycling Solutions durchgeführten Studie, die ergab, dass 34 % der entsorgten Festplatten noch vertrauliche Daten enthielten.

Deshalb ist es äußerst wichtig, zu wissen, dass es drei Typen der Festplattenformatierung gibt, die Low-Level-Formatierung, die Schnellformatierung und die vollständige Formatierung. Sie alle haben unterschiedliche Funktionsweisen.

- **Low-Level-Formatierung:** Diese umfasst die Einteilung des Laufwerks auf unterster Ebene in Spuren und Sektoren, um sie auf die Werkeinstellungen zurückzusetzen. Hierbei handelt es sich um einen zeitaufwendigen, aber effektiven Prozess, der allerdings nur selten angewendet wird. Häufiger werden die Schnell- und die vollständige Formatierung genutzt.
- **Schnellformatierung:** Diese Methode stellt den Metadatenbereich des Laufwerks wieder her, um zusätzlichen Speicherplatz zu schaffen, löscht die Daten allerdings nicht.
- **Full Reformatting:** Die Hauptfunktion der vollständigen Formatierung ist die Untersuchung aller Sektoren des Laufwerks, darunter auch der beschädigten Sektoren, deren Neueinteilung und die anschließende Löschung aller aktiven Daten. Die Ergebnisse können je nach Betriebssystem variieren.

Holger Engelland zufolge, Manager des Datenrettungslabors bei Kroll Ontrack, „kann die Formatierung zur sicheren Datenlöschung zu unterschiedlichen Ergebnissen führen, da jedes Betriebssystem den Vorgang auf unterschiedliche Weise ausführt. Um Daten erfolgreich bis zu einem Zustand zu löschen, aus dem sie nicht wiederhergestellt werden können, muss man die Daten mit renommierter Löschsoftware vollständig überschreiben."

Ungeduld kann ein unsichtbarer aber ausschlaggebender Übeltäter bei der Löschung von Festplatten sein.

Die Untersuchung der Festplatten und Solid State Drives ergab, dass bei 11 % der Festplatten eine unvollständige Löschung durchgeführt wurde, sodass darauf eine beträchtliche Menge an Daten zurückgeblieben war, die nur darauf warteten, offengelegt zu werden. Auch wenn der genaue Grund nicht ermittelt werden kann, ist anzunehmen, dass Nutzer durch die Dauer, die die Löschung ihrer Laufwerke in Anspruch nimmt, ungeduldig geworden sind. In Anbetracht dessen, dass die Löschung einer 500-GB-Festplatte bis zu sieben Stunden dauern kann, ist das sogar verständlich. Außerdem kann eine unvollständige Bereinigung auf einen weitergehenden Fehler bei der angewendeten Löschmethode zurückgehen.

Private wie geschäftliche E-Mails, Geschäftspräsentationen, sensible Finanzdokumente, vertrauliche Unternehmensdokumente, Fotos, Videos – all das erstellen, speichern und teilen wir über das digitale Universum. Die Herausforderung dabei ist, dass die meisten keine Technik-Genies, Datenschutzgurus oder Spezialisten auf dem Gebiet der Datenwiederherstellung sind. Sie verfügen nicht über ausreichendes Wissen, entsprechende Fähigkeiten und die nötige Erfahrung, um vollständig zu verstehen, mit welchen Löschmethoden Daten wirklich für immer vernichtet werden können – und mit welchen nicht. Leider gehen vor allem Einzelpersonen sowie Unternehmen von einer Reihe falscher Annahmen aus, die zu einer Vielzahl gefährlicher Szenarien, wie Identitätsdiebstahl, Internetbetrug oder öffentliche Bloßstellung, führen können. Eine dieser Annahmen ist, dass alle Löschmethoden gleich wirksam bei der Datenvernichtung sind. Wie wir in dieser Studie zeigen konnten, ist das jedoch nicht der Fall.

Die beste Methode zur sicheren Löschung von Laufwerken, insbesondere von SSDs, ist die zufällige Überschreibung mithilfe von Löschsoftware. Interessanterweise wurde diese Methode nur bei sechs Prozent der Festplatten und Solid-State-Drives aus unserer Studie durchgeführt. In jedem Fall erwies sich die zufällige Überschreibung jedoch als hundertprozentig wirksam und hinterließ keinerlei Daten auf den Laufwerken. Unternehmen wie auch Verbrauchern wird empfohlen, sich über die Effektivität der unterschiedlichen Datenlöschmethoden und die zahlreichen Lösungen zum Schutz ihrer Daten und Privatsphäre zu informieren.

Was können Sie tun, um Ihre Daten zu schützen?

Bevor Sie Ihr Mobilgerät verkaufen:

- Eruieren Sie den Wert Ihres aktuellen Mobilgeräts. Die Vorbereitung eines Mobilgeräts für den Wiederverkauf nimmt Zeit in Anspruch und zieht gegebenenfalls zusätzliche Kosten für die ordnungsgemäße Löschung nach sich. Eine Abwägung des Wiederverkaufswerts gegen die Anschaffungskosten kann dabei helfen, eine fundierte Entscheidung für oder gegen den Verkauf zu treffen.
- Informieren Sie sich über die Rückkaufsangebote von Händlern und Online-Marktplätzen, wie Amazon, eBay und Gazelle.com. Finden Sie heraus, wie der Prozess funktioniert und welche Verkaufsgebühren anfallen.
- Wenn Sie Ihr privates Mobilgerät für die Arbeit nutzen (BYOD-Programm), informieren Sie sich über die Richtlinien Ihres Unternehmens zur Datenspeicherung und den BYOD-Wiederverkaufsrichtlinien für diese Art von Geräten.
- Sichern Sie sämtliche Daten, die wichtig für Sie sind oder die Sie in Zukunft für ein anderes Gerät, eine andere Festplatte oder Cloud-Plattform benötigen könnten.
- Machen Sie eine Bestandsaufnahme aller unterschiedlichen Datentypen, die Sie über Ihr Mobilgerät erstellt, angelegt, gespeichert und geteilt haben. Eine solche Liste wird Ihnen beim Querverweis nach der Löschung Ihrer Daten helfen.
- **Löschen Sie Ihre Daten zuverlässig:**
  - Nutzen Sie bei einem Android-Gerät die Geräteeinstellungen, um die Daten zu verschlüsseln, und führen Sie anschließend eine werkseitige Löschfunktion aus. Alle Restdaten bleiben in verschlüsselter und unbrauchbarer Form zurück.
  - Entfernen Sie die Mikro-SD-Karte (falls vorhanden) bzw. verkaufen Sie sie nicht mit.
  - Verwenden Sie bei einem iOS-Gerät die iOS-Wiederherstellungsfunktion, um die Werkeinstellungen wiederherzustellen, oder nutzen Sie „Inhalte & Einstellungen löschen" im iPhone-Menü. Beide Optionen löschen den dem Gerät zugeordneten Verschlüsselungscode, wodurch gegebenenfalls zurückbleibende Daten nicht wiederhergestellt werden können.
  - Für alle Mobilgeräte ist bewährte Löschsoftware die beste Lösung zur sicheren Löschung aller Daten. Finden Sie heraus, welche Software speziell auf Mobilgeräte zugeschnitten ist und ein Löschzertifikat bietet.
- Wenn Sie eine externe SD-Karte zur Übertragung von Daten auf ein anderes Gerät genutzt haben oder um die Speicherkapazität Ihres Geräts zu erhöhen, löschen Sie auch hiervon die Daten. Für eine zuverlässige Löschung einer SD-Karte, sodass die Daten nie wieder sichtbar werden, müssen Sie die SD-Karte zunächst aus dem Gerät entfernen und anschließend in einen Computer einstecken. Dieser kann alle ihre Sektoren korrekt erfassen und führt anschließend eine Software aus, um alle Daten sicher zu löschen.
- Stellen Sie sicher, dass die Datenlöschmethode den gesetzlich vorgeschriebenen Überschreibungsstandards wie HMG Infosec und DoD 5220.22 M entspricht und sie außerdem von Regierungsbehörden und Organisationen, wie der NATO, dem Verteidigungsministerium der Vereinigten Staaten, CESG, TÜV SÜD und DIPCOG, zugelassen ist.
- Fordern Sie einen Löschnachweis an. Hierbei sollte es sich um ein manipulationssicheres Zertifikat handeln, das nicht nachträglich geändert werden kann. Betrachten Sie es wie einen Prüfpfad bei der Steuererklärung. Damit wird der Schutz der Privatsphäre des Wiederverkäufers und außerdem die dem Käufer Ihres gebrauchten Geräts geschuldete Sorgfalt gewährleistet.
- Prüfen Sie genau, dass wirklich alle Daten gelöscht wurden. Berufen Sie sich auf Ihre Datentypenliste dieser Checkliste. Sollte der Wiederverkäufer keinen Löschnachweis gewährleisten können, stehen kostenlose Datenwiederherstellungslösungen zur Verfügung, um Ihr Gerät zu prüfen.

Bevor Sie Ihre Festplatte oder Ihr Solid State Drive verkaufen:

- Eruieren Sie den Wert Ihrer Festplatte oder Ihres Solid State Drive, bevor Sie sie verkaufen.
- Sichern Sie alle wichtigen Daten auf einem anderen Laufwerk oder Gerät.
- Löschen Sie Ihr Laufwerk zuverlässig mithilfe einer der folgenden Methoden:
  - **Low-level Format Only:** Verlassen Sie sich für eine sorgfältige Bereinigung Ihres Laufwerks nicht auf eine vollständige oder Schnellformatierung.
  - **Datenüberschreibung:** Dies ist die beste Methode für SDDs und HDDs. Bei der Wahl einer Löschsoftware zur Überschreibung gehen Sie folgendermaßen vor:
    - Finden Sie heraus, ob die Software die richtige Löschmethode für Ihren Laufwerktyp durchführen kann.
    - Finden Sie heraus, wie viele Überschreibungsdurchläufe die Löschsoftware insgesamt durchführt. Bei jedem Durchlauf wird das Laufwerk vollständig mit Nullen, Einsen oder zufälligen Daten überschrieben. Nach der „Kurz"-Spezifikation des Verteidigungsministeriums der Vereinigten Staaten und vieler anderer Militärs weltweit sind drei Durchläufe ausreichend.
    - Stellen Sie sicher, dass das Unternehmen bereit ist, in Form eines manipulationssicheren Zertifikats über alle Löschungen die Effektivität seiner Software schriftlich festzuhalten.
  - **Kryptografische Löschung:** Verschlüsseln Sie alle Daten auf dem Laufwerk, prüfen Sie, ob alle Daten verschlüsselt sind und überschreiben und löschen Sie anschließend den Verschlüsselungscode.
- Stellen Sie sicher, dass die Datenlöschmethode den oben beschriebenen gesetzlich vorgeschriebenen Überschreibungsstandards entspricht und sie außerdem von Regierungsbehörden und Organisationen zugelassen ist.
- Fordern Sie einen Löschnachweis an. Hierbei sollte es sich um ein manipulationssicheres Zertifikat handeln, das nicht nachträglich geändert werden kann.
- Prüfen Sie genau, dass wirklich alle Daten gelöscht wurden. Genau wie bei Mobilgeräten handelt es sich hierbei um einen sehr wichtigen Schritt. Sollte der Wiederverkäufer keinen Löschnachweis gewährleisten können, stehen kostenlose Datenwiederherstellungslösungen zur Verfügung, um Ihr Gerät zu prüfen

Schlussfolgerung

Datenschutz spielt eine immer größere Rolle in unserem Alltag. Es wird nahezu täglich in den Nachrichten und in unserem Umfeld über betriebliche Datenschutzverletzungen und Datendiebstahl bei Verbrauchern berichtet. Laut einer aktuellen Studie des Identity Theft Resource Center (ITRC) erreichte die Anzahl an Datenschutzverletzungen in den USA im Jahr 2014 ein Rekordhoch von 783 (durchschnittlich 15 Datenschutzverletzungen pro Woche).

Angesichts der weltweiten Verbreitung von Datenschutzproblemen setzen sich zu viele Verbraucher und Unternehmen einem Risiko aus, indem sie keine wirksamen und bewährten Methoden zum Schutz ihrer Informationen vor dem Wiederverkauf ihrer Mobilgeräte und Laufwerke anwenden. Cyber-Diebstahl und Hacking betrifft nicht mehr nur Computer und Server. Raffinierte Hacker können im Internet ganz einfach günstige, gebrauchte Wiederherstellungssoftware finden, mit denen sie wertvolle Daten stehlen können.

Selbst die kleinste Menge an Daten kann genügend Personen- oder vertrauliche Unternehmensdaten enthalten und irreparable Schäden verursachen. Diese Daten können auf unterschiedlichen Wegen weiterverwendet werden: Beim Online-Kauf mit gestohlenen Kreditkarteninformationen, zur Anmeldung einer neuen Kreditlinie mit Personen- oder Unternehmensdaten, zur Erpressung von Lösegeld von Personen oder Firmen unter der Drohung der Weitergabe sensibler Informationen oder Schlimmeres. Der Ideenreichtum der Cyber-Kriminellen ist grenzenlos.

Ob Smartphone, Tablet oder Festplatte – sämtliche Daten, personen- oder firmenbezogen, sollten vor dem Verkauf oder der Entsorgung vollständig und sicher gelöscht werden. Andernfalls besteht das Risiko, dass sensible Informationen in die falschen Hände gelangen und Ruf- oder Finanzschäden und Rechtsverletzungen nach sich ziehen. Zeit in die Recherche nach effektiven Datenlöschmethoden zu investieren, ist weitaus gewinnbringender, als darauf zu warten, das nächste Opfer einer Datenschutzverletzung zu werden.

Über Blancco Technology Group

Blancco Technology Group ist Weltmarktführer für Datenlösch- und Diagnosemanagement. Wir unterstützen mit unserer bewährten und vielfach zertifizierten Software Kunden bei Tests, Diagnosen, Reparaturen und der Wiederaufbereitung- und Verwendung von IT-Geräten. Unser Kundenkreis besteht aus Weltkonzernen unterschiedlichster Branchen, Geräteherstellern, Mobilfunknetzbetreibern, Händlern, Finanz- und Gesundheitswesen, Dienstleistern, sowie Regierungsorganisationen weltweit. Die Blancco Technology Group hat ihren Hauptsitz in Alpharetta, GA, USA und ist weltweit vertreten.

Blancco, ein Geschäftsbereich der Blancco Technology Group, ist der weltweite Industriestandard für zertifizierte Datenlöschung. Wir bieten tausenden Organisationen Schutz vor kostspieligen Sicherheitsverletzungen und stellen, durch eine 100 % manipulationssichere Nachverfolgung, die Einhaltung internationaler Standards sicher.

SmartChk, entwickelt von XCaliber Technologies, einem Geschäftsbereich der Blancco Technology Group, ist weltweit der Pionier am Markt für Mobilgerätdiagnostik und Business Intelligence. Wir bieten unseren Kunden optimale Test-, Diagnose- und Reparaturmöglichkeiten für Mobilgeräte an, um ihre Kundenerfahrung zu verbessern. SmartChk (oder Xcaliber Technologies) gewährleistet erstklassige Unterstützung von der Implementierung bis hin zur individuellen Prozessoptimierung. Für weitere Informationen, besuchen Sie uns unter www.blanccotechnologygroup.com und folgen uns auf Twitter unter @BlanccoTech.

Über Kroll Ontrack

Kroll Ontrack ist Weltmarktführer im Bereich Datenwiederherstellung und bietet Rechtsbehörden, Unternehmen und Regierungseinrichtungen sowie Verbrauchern technologiegetriebene Services und Software zur effizienten und kostengünstigen Wiederherstellung, Suche, Analyse, Erstellung und zum Management von Daten.

Mit weltweit 18 Reinraumlaboren in den wichtigsten Regionen weltweit und erstklassigem Ingenieurwissen sowie über 25 Jahren Erfahrung bietet Kroll Ontrack erfolgversprechende Lösungen für alle Arten der Datenwiederherstellung und Datenvernichtung.

Service und Software zur Datenwiederherstellung: Stellen Sie Daten auf Datenbändern, Festplatten, Mobilgeräten, in virtuellen Umgebungen, Betriebssystemen und einer Vielzahl von anderen Speichergeräten über Labor-, Fern- und Do-It-Yourself-Funktionen wieder her.

Service und Software zur Datenlöschung: Löschen Sie dauerhaft alle Datenspuren von Medien und schützen Sie sensible Informationen vor der Entsorgung mit Do-It-Yourself-Löschsoftware und Datenvernichtungsdiensten.

Ontrack® PowerControls Software: Suchen, sammeln, verwalten und wiederhstellen von Daten in Umgebungen mit Microsoft® Exchange, Microsoft® Office SharePoint® oder Microsoft® SQL Server®.

Für weitere Informationen über Kroll Ontrack und unser Angebot, besuchen Sie uns unter: www.krollontrack.de oder folgen Sie @KrollOntrackD auf Twitter.

blancco technology group

KrollOntrack™ By KrolLDiscovery