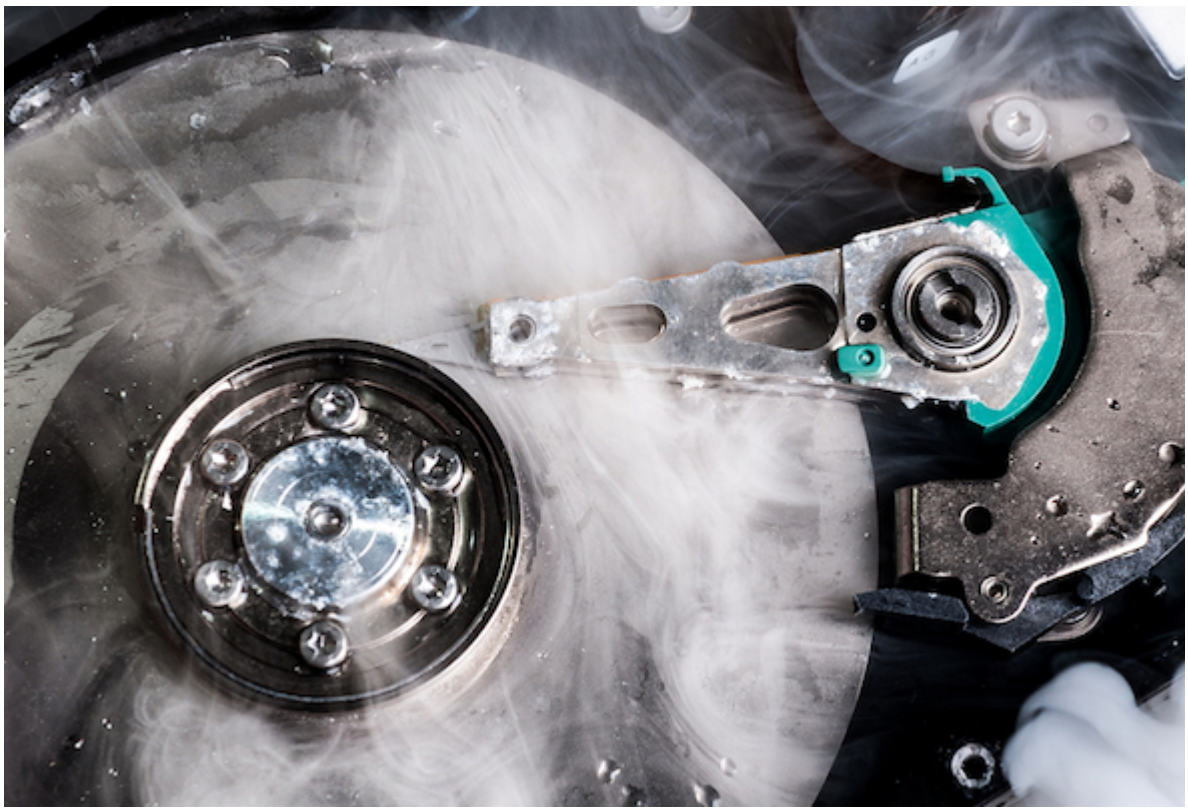
Wie man Festplatten auch selbst vernichten kann ...

vparthier



… und wie man Daten auf Festplatten, SSDs und Flash-Medien löschen kann! Für eine physische Zerstörung von klassischen Magnet-Festplatten – auch HDD genannt – bedarf es nicht unbedingt eines externen Dienstleisters.

Mit ein wenig Werkzeug lässt sich bereits mit einfachen Mitteln eine ausreichende Vernichtung der Datenträgerscheiben bzw. Platter erzielen, die eine professionelle Datenrettung unwirtschaftlich machen.

Nicht nur Ministerien sondern auch Unternehmen und private Anwender stehen bei einem Systemwechsel vor dem Problem: Was passiert mit den alten Datenträgern, die in der Regel auch Daten enthalten, welche nicht in falsche Hände geraten sollten?

Datenretter arbeiten in mancher Hinsicht wie Archäologen: Kein Bit ist ihnen zu wertlos, als dass man nicht alles tun würde, um es zu retten. Festplatten und andere Datenträger „sicher“ zu löschen, damit die Daten auch von einem Profi nicht mehr rekonstruiert werden können, darf nicht unbedacht bleiben. Denn kaum etwas ist in unserer digitalen Welt gefährlicher als sensible Daten, die unzerstört das Haus verlassen und dann möglicherweise in falsche Hände gelangen.

Datenvernichtung durch Programme

Eine Vielzahl an kommerziellen Löschprogrammen verspricht nicht weniger als das komplette und rückstandsfreie Löschen von Datenträgern. Oft bleibt es jedoch leider beim Versprechen, was weniger an der (sehr wohl auch) unterschiedlichen Qualität dieser Programme liegt, sondern daran wie Festplatten und Flash-Speicher wie SSDs, USB-Sticks und SD-Cards aufgebaut sind.

Geheime Bereiche auf Datenträgern

Um zu verstehen, warum das rückstandsfreie Löschen praktisch ein Ding der Unmöglichkeit ist, muss man zunächst wissen, wie moderne Datenträger arbeiten. Ein großes Problem beim Datenlöschen sind etwa jene Bereiche, die im Laufe des Betriebes fehlerhaft werden können. Wann immer in einem Bereich ein Defekt auftritt, wird dieser abgetrennt und die Daten in einen Ersatzbereich kopiert. Auf diese gesperrten Regionen kann das System nicht mehr zugreifen – also auch nicht eine dafür ungeeignete Löschsoftware. Die ursprünglichen Daten sind jedoch dort immer noch vorhanden und können von professionellen Datenrettern mit speziellen Verfahren ausgelesen werden.

Bedenkt man, dass bei einem Medium mit einem Terabyte Speicherplatz die Reservebereiche mehrere 100 MB ausmachen, kann man ermessen, wie viele Dateien sich der Löschung entziehen können.

Eine besondere Problematik tritt bei SSDs, USB-Sticks und SD-Karten auf, da durch „wear-levelling“ Rohdaten an immer unterschiedlichen physischen Adressen gespeichert werden. Flash-Speicher verfügen über deutlich mehr Reservespeicher als Festplatten, da die Lebensdauer der einzelnen Flash-Zellen verhältnismäßig kurz ist. Die Daten werden auf einzelnen Zellen so verteilt, dass diese möglichst alle eine gleiche Anzahl von Schreib-Zyklen aufweisen. Dadurch wird vermieden, dass Bereiche, auf die häufiger Schreib-Zugriffe erfolgen, früher defekt werden. Somit werden bei einmaligem Überschreiben eines Flash-Datenträgers nie alle Daten vernichtet.

Datenvernichtung durch mehrfaches Überschreiben von Datenträgern

Ein gerne kolportiertes Missverständnis ist übrigens, dass wiederholtes Überschreiben die Löschung einer Magnet-Festplatte sicherer macht. Das beruht auf jahrzehntealten Platten-Designs, die noch mit nicht überlappenden Spuren funktionierten. Bei modernen Festplatten hat sich die Aufzeichnungsdichte derart verändert, dass einmaliges Überschreiben ausreicht, um eine Wiederherstellung der überschriebenen Sektoren zu verhindern.

Das Credo von Nicolas Ehrschwendner, Geschäftsführer der Attingo Datenrettung GmbH, lautet somit: „Die Frage ist nicht wie oft man die Daten überschreibt, sondern ob man tatsächlich alle Bereiche überschrieben hat. Ist ein einzelner Sektor einmal mit Daten überschrieben, so ist dieser auch nicht mehr rekonstruierbar.“

Selbstzerstörung

Moderne Datenträger verfügen meistens über einen standardisierten Befehl zur Selbstvernichtung. Wird dieser ausgeführt, sollte der Datenträger alle Daten – auch die Reservebereiche – vollständig vernichten. Die Problematik ist jedoch vielschichtig: Immer wieder ist der Befehl nicht korrekt implementiert oder der Datenträger zeigt bereits erste Defekte und die Selbstzerstörung ist infolgedessen nicht vollständig. Wiederum gilt, dass eine Verifikation einer erfolgreichen Datenvernichtung durch den Anwender quasi unmöglich ist.

Physische Zerstörung von Datenträgern

Abseits der auf Software basierenden Verfahren wollen wir jetzt ein bisschen brachiale Gewalt walten lassen, die man mit entsprechender Vorsicht auch selbst umsetzen kann. Der Datenträger ist nach diesen Methoden unbrauchbar und kann auch nicht weiter verwendet werden.

Shreddern und Zermahlen

Beginnen wir mit den wirklich schweren Geschützen: Shreddern und Mahlen des Datenträgers kann als eine der sichersten Methoden der Datenvernichtung angesehen werden.

Bei Festplatten nimmt ein Datensektor typischerweise nur wenige Mikrometer auf der Oberfläche ein, so sind kleine Bruchstücke theoretisch mit Hilfe von Rastersondenmikroskopen noch auslesbar. Allerdings hat weltweit noch kein Datenretter diese Theorie jemals in die Praxis umsetzen können, dies scheitert mitunter auch an dem nötigen Budget für diese jahrelange Arbeit.

SSDs sowie andere Flash-Datenträger bestehen aus einem oder mehreren Flash-Chips. Bei einer mechanischen Datenvernichtung müssen alle verbauten Flash-Chips (Wafer) zerstört werden. Auch hier sollte die Korngröße beim Schreddern kleiner als die minimale Größe der in den Chips eingegossenen Wafer sein, ein Millimeter Kantenlänge sollte hier hinreichend klein sein.

Bohren, Flexen oder Hämmern

Da die kleinen Bruchstücke eines Platters eben nur noch theoretisch rekonstruierbar sind, reicht es in den meisten Fällen auch aus die Magnetscheibe soweit zu beschädigen, dass ein normales Auslesen als Festplatte nicht mehr möglich ist. Hierzu bieten sich drei einfache Methoden, die wir auch im Video demonstrieren:

1. Die Magnetscheiben mit einem Bohrer mehrfach durchlöchern. Wichtig ist hier in der Festplatte auch tatsächlich die Platter zu treffen und nicht nur im Bereich der Schreib/Leseköpfe Unheil anzurichten.
2. Die Magnetscheiben mit einer Trennscheibe oder einem Winkelschleifer durchtrennen. Wichtig ist hier alle einzelnen Platter zu zerschneiden.
3. Die Magnetscheiben mit einem Hammer zu deformieren. Im Falle von Glas-Scheiben zerspringen diese bei der ersten Berührung in viele Einzelteile, bei

Aluminium-Scheiben erfolgt nur eine Deformierung, wobei auch hier wieder jede Scheibe einzeln zu bearbeiten ist.

Datenvernichtung durch Rösten?

Eine weitere Methode wäre das Verbrennen der Festplatte. Jedes magnetische Material hat eine spezifische Temperatur, die sogenannte „Curie-Temperatur“, ab welcher sich die Elementar-Magnete von selbst wieder in zufällige Richtungen ausrichten. Damit wird jeder gerichtete Magnetismus in dem Material beseitigt, was eine sichere Vernichtung der Daten gewährleistet. Die Curie-Temperatur der üblichen magnetischen Materialien bei Festplatten liegt in einem Bereich, welcher 800°C überschreitet, eine Temperatur, mit der das heimische Backrohr sicherlich überfordert ist. Das bedeutet, dass solche Vernichtungen in speziellen Öfen durchgeführt werden müssten.

Bei SSDs und anderen Flash-Speichern genügen in der Regel einige 100°C, jedoch sollte die Hitzeeinwirkung über einen längeren Zeitraum stattfinden, damit die Daten wirklich vollständig vernichtet sind.

Der Riesenmagnet

Eine ebenfalls sichere Methode der endgültigen Datenvernichtung – jedoch nur bei HDD Festplatten und Tapes - besteht im Entmagnetisieren der magnetischen Oberflächenbeschichtung durch ein ausreichend starkes Magnetfeld. Kommerzielle Geräte, die solche Magnetfelder herstellen, werden unter dem Begriff „Degausser“ angeboten.

Löschen? Zerhacken? Verschlüsseln!

Eine sichere und weniger destruktive Methode ist die Datenverschlüsselung, da hier das Problem sozusagen an der Wurzel gepackt wird. Wenn man Daten schon nicht so einfach sicher löschen kann, liegen sie dann wenigstens so vor, dass sie auch von Spezialisten nicht mehr genutzt werden können: nämlich verschlüsselt. Dies gilt allerdings nur so lange wissenschaftlich aktuell anerkannte und korrekt implementierte Verschlüsselungsverfahren eingesetzt werden, und die Passwörter eventuellen Datenschnüfflern nicht bekannt sind. Bei der vorherrschenden Kreativität in diesem Bereich liegt ja bekanntlich einiges im Argen, wie illustre Passwörter á la „12345“ immer wieder belegen.

Ein Vorteil der Verschlüsselung ist, dass auch bei einem Diebstahl eines Laptops etwa ein Zugriff durch Unbefugte nicht möglich ist. Allerdings hat die Verschlüsselung auch einen handfesten Nachteil: Geht der Verschlüsselungs-Key verloren, ist es in den meisten Fällen nicht mehr möglich, Zugriff auf die eigenen Daten zu erlangen – man hat sich also selbst „ausgesperrt“ und alle Daten sind verloren.

Wenn man wirklich sicher gehen will

Daher bleibt bei heiklen Daten nur eine Alternative: Den Datenträger von Anbeginn der Nutzung verschlüsseln, dann die Daten vollständig überschreiben

und im Anschluss diese Löschung einer Zertifizierung durch einen professionellen Datenretter unterziehen oder noch eine physische Zerstörung anwenden.

Das sollte dann auch wirklich ausreichend sein!

www.attingo.com/de