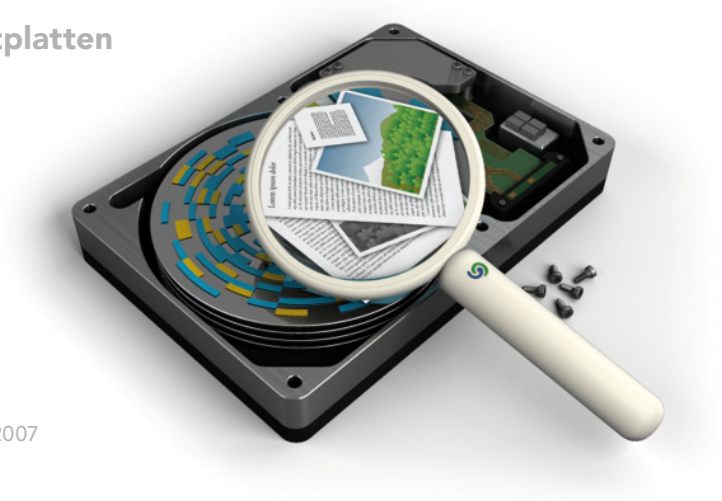
Studie zum Datenschutz bei gebrauchten Festplatten

Deutschland Deine Daten



Dipl.-Inform. Olaf Kehrer • O&O Software GmbH, Berlin • September 2007

Studie zu Datenschutz und Datensicherheit bei gebrauchten Festplatten und Speicherkarten in Deutschland und den USA

Löschen heißt nicht, dass die Daten vernichtet sind. Die Tatsache, dass dieses vielen Anwendern von Computersystemen und Digitalkameras nicht bekannt ist, hat erneut zu erschreckenden Ergebnissen dieser Studie geführt. Bei unseren Probekäufen bei Online-Auktionen konnten wir auf vermeintlich gelöschten Datenträgern in den meisten Fällen sehr persönliche und auch berufliche Daten wiederherstellen. Zwei Drittel der Speichermedien enthielten noch die Daten der Vorbesitzer. Fast alle Betroffenen waren davon überzeugt, dass sie die Daten zuvor gelöscht hatten. Aber kaum einer weiß, dass das Löschen mit Windows oder einer Digitalkamera nicht gleichzusetzen ist mit deren endgültiger Vernichtung. In dieser Studie sollen über die Ergebnisse hinaus mögliche Ursachen und Hintergründe dieser Problematik beleuchtet werden. Darüber hinaus werden ausführlich Lösungsmöglichkeiten dargestellt, um die unwissentliche Weitergabe von vertraulichen Daten zu verhindern.

Die Einführung von Windows Vista stellt vollkommen neue Anforderungen an die Hardware der Rechner. Viele PC-Besitzer müssen ihre Rechner aufrüsten oder gleich einen neuen Computer kaufen. Was passiert aber dann mit dem alten Rechner? Im privaten Umfeld wird er vielleicht verkauft oder einfach verschenkt. Unternehmen mustern ihre Rechner aus und geben sie entweder an Leasinggeber zurück oder veräußern sie. Wissen sie aber auch, dass man Daten von nicht sicher gelöschten Festplatten mit ein paar Mausklicks einfach wiederherstellen kann? Private und Unternehmensdaten können so unbemerkt den Besitzer wechseln und großen Schaden anrichten.

Im Rahmen unserer Studie haben wir in den Jahren 2006 und 2007 fast 400 Datenträger ersteigert und darauf untersucht, ob sie noch Daten enthielten oder ob sie sicher gelöscht worden waren. Mehr als 66 % der Festplatten waren nicht gelöscht, so dass die Daten der Vorbesitzer mit speziellen Datenrettungsprogrammen wiederhergestellt werden konnten.

Im Zeitalter des Internets ist Sicherheit ein großes und populäres Thema. Immer wieder wird auf Angriffe beim Online-Banking durch Phishing hingewiesen. Häufig wird in Tageszeitungen vor sich schnell verbreitenden E-Mail-Viren gewarnt, so dass die meisten Anwender für dieses Thema immer sensibler geworden sind. Auch das Sammeln und Ausspähen von Benutzerdaten durch sogenannte Spyware rückt immer stärker in das öffentliche Interesse und beschäftigt vermehrt auch die Strafverfolgungsbehörden.

Doch was passiert mit den eigenen privaten oder geschäftlichen Daten, wenn man seinen Rechner nicht mehr braucht? Wenn man ihn verkauft oder verschenkt? Vielen Anwendern ist nicht bewusst, dass sie ohne besondere Sicherheitsvorkehrungen leichtfertig ihre Daten aus der Hand geben und damit Informationen preisgeben, die ihnen großen Schaden zufügen können.

Studie

Für diese Studie haben wir in den vergangenen 18 Monaten insgesamt 395 Datenträger bei Online-Auktionen erworben und ausgewertet. Darunter waren 80 Festplatten aus den Vereinigten Staaten, da wir die Sensibilität der dortigen Anwender mit der der hiesigen vergleichen wollten.

Die erworbenen Festplatten hatten eine Gesamtkapazität von mehr als 15 Terabyte (15.116 GByte). Von den 280 Festplatten waren 59 technisch defekt, was einer Quote von 21 % entspricht. Defekte Festplatten wurden nicht weiter betrachtet, da zu ihrer Rekonstruktion ein erhöhter Aufwand notwendig gewesen wäre. Diese Möglichkeit würde einem normalen PC-Nutzer nur eingeschränkt zur Verfügung stehen und ist daher für diese Studie nicht relevant.

Sensibilisiert durch den Fund unzähliger Fotos von Privatpersonen haben wir die Analyse vermeintlich gelöschter Datenträger ausgeweitet und 115 Speicherkarten, USB-Sticks und Digitalkameras ersteigert. Diese Speichermedien waren erstaunlicherweise allesamt technisch intakt und konnten somit analysiert werden.

Ergebnisse
Von den verbleibenden 221 Festplatten waren 72 sicher gelöscht, so dass keine Daten rekonstruiert werden konnten. Dies entspricht rund 33 %. Die restlichen 149 Festplatten waren entweder gar nicht gelöscht oder nur formatiert worden.

Dies bedeutet, dass 67 % der Festplatten persönliche und geschäftliche Daten enthielten, die rekonstruiert werden konnten. Insgesamt wurden über 17 Millionen Dateien mit einer Gesamtgröße von 2,4 Terabyte auf den Festplatten wiederhergestellt. Darunter waren große Mengen an Word-Dokumenten und Excel-Tabellen sowie circa 60 E-Mail-Postfächer mit dem gesamten Mailverkehr der Vorbesitzer. Hinzu kam eine riesige Masse an privaten Fotos und Videos, die teilweise pornographische Inhalte hatten.

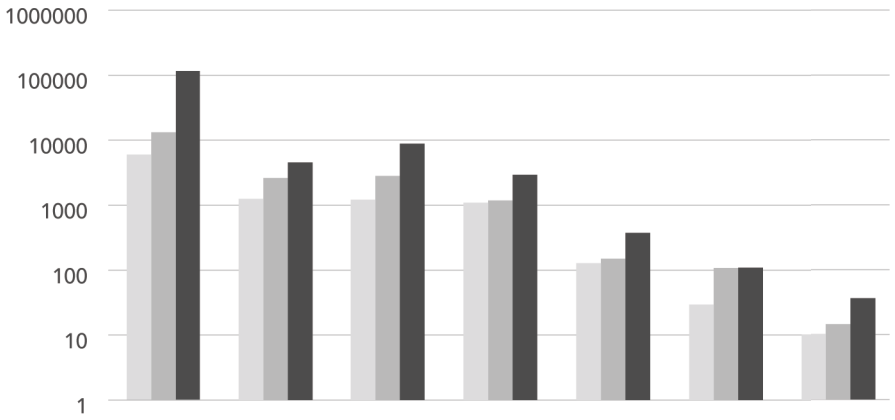
Von den 115 Speicherkarten, USB-Sticks und Digitalkameras waren 32 sicher gelöscht, was einer Quote von 27,8 % entspricht. Von 83 Speichermedien ließen sich Daten wiederherstellen, was 72,2 % entspricht.

Abbildung 1: Gefundene Dateien pro Festplatte

Insgesamt konnten über 17 Mio. Dateien wieder hergestellt werden (2005: 3,3 Mio., 2004: 590.000). Hiervon entfiel erneut der größte Teil auf Grafik- und Internetseiten (GIF, JPEG, HTML).

Die Grafik zeigt die durchschnittliche Anzahl der gefundenen Dateien pro Datenträger. Dabei wurden die Gesamtzahlen der gefundenen Dateitypen durch die Anzahl funktionstüchtig Datenträger dividiert.

y-Achse der Tabelle ist logarithmisch aufgetragen



	Gesamt	GIF	JPEG	HTML	Word	Excel	E-Mail
Anzahl 2004	7867	1988	1889	1047	204	53	17
Anzahl 2005	29511	3166	3179	1577	354	130	21
Anzahl 2007	114108	6409	9778	4604	581	135	66

Auszüge aus den rekonstruierten Daten
Aus der gewaltigen Anzahl an rekonstruierten persönlichen und geschäftlichen Daten stellen wir im Folgenden ein paar Fälle exemplarisch vor. Alle diese Daten sind entweder sehr privat oder vertraulich, woraus wir schließen, dass der ursprüngliche Eigentümer sie ganz sicher nicht der Öffentlichkeit preisgeben wollte.

Petze, Petze, ging in Laden …
Der erste Fall ist eine Festplatte, die diverse persönliche Dokumente enthielt. Darunter war ein Textdokument, das ein Anschreiben an den Deutschen Rentenbund (vormals Bundesversicherungsanstalt für Angestellte) enthielt. Darin wird ein anscheinend für arbeitsunfähig erklärter Frührentner beschuldigt, schwarz zu arbeiten; dabei wird dessen komplette Anschrift und das Geburtsdatum angegeben, um der Behörde die Suche zu erleichtern. Es ist wohl stark anzunehmen, dass weder der Absender noch der Empfänger öffentlich bekannt werden möchte.

Sehr geehrte Damen und Herren,

immer wieder sehe ich es wie es notdürftigen Leuten einfach an Mitteln fehlt weil die kleine Rente die sie erhalten vorne und hinten nicht reicht und diese Menschen auch nicht mehr die Gelegenheit haben sich nebenbei etwas dazu verdienen können. Wenn ich aber sehe, dass es Frührentner gibt die mit ihren 43 Jahren eigentlich **Kern Gesund** sind und einer Nebentätigkeit nachgehen die einer ca. **30Std.** Woche entspricht ggf. mehr, dieses nur zum Teil über die Steuerkarte laufen lassen, den Rest sich dann ***SCHWARZ*** ausbezahlen lassen auf ein anderes **Sparkonto** und dann vom Staat noch alles bekommen platzt mir wirklich der Kragen!

Es ist doch unvorstellbar das jemand, bei dem man vor ein paar Jahren oder so den ein Krankheitsbild festgestellt hat und damals gleich gesagt hat das man besser in Rente gehen kann und dem Arbeitsmarkt nicht mehr zur Verfügung steht! Und was noch viel schlimmer ist, dem jenigen wird auch noch fast alles Geschenkt bzw. für ihn bezahlt oder nur zum teil angerechnet! Ich rede nun von Kleinigkeiten wie Telefon, Kabelanschluss, Fahrkarten usw. Das es da noch einige Leute ausnutzen und sich da noch ein schönes Leben von machen können finde ich eine Frechheit! Zumal diese Gesundheitlich **Topfit** sind und ja auch neben ihrer Rente noch bestimmt das **Doppelte dazu verdienen**! Andere müssen dafür meist immer Überstunden schieben um sich dies Leisten zu können, während andere nur die Hand aufhalten brauchen! Komisch das der BfA dies noch nie aufgefallen ist oder noch niemand etwas davon gewittert hat! Abgesehen von den anderen Skurrilen Internet-Geschäften die zusätzlich noch dazu kommen.
Ich habe diese Informationen aus meinem Bekanntenkreis bekommen und ich bin fast vom Stuhl gefallen als mir dies alles zugetragen wurde.

Ich bitte Sie diese **Angelegenheit zu prüfen** zu mindestens im **Interesse der BfA** und der dadurch entstehenden **unnötigen kosten für die BfA und letzt endlich der Steuerzahler**:

Abbildung 2: Anschreiben an den Deutschen Rentenbund (vormals BfA) mit Hinweis auf einen Schwarzarbeiter (Speichermedium: Festplatte)

Von dem „Anschwärzer" war auch gleich noch das Bewerbungsschreiben auf der Festplatte vorhanden. Sicherlich ist auch dies ein Dokument, das er nicht in falschen Händen sehen möchte.

Bitte senden Sie uns Ihre Bewerbungsunterlagen!
Wenn man sich um einen Arbeitsplatz bemüht, dann muss man entsprechende Unterlagen einreichen. Diese erstellen heutzutage die meisten am PC, denn damit erreicht man ein gutes Erscheinungsbild und man kann die Unterlagen später auch noch erweitern und wiederverwenden. Diese Vorteile kehren sich aber in einen entscheidenden Nachteil um, wenn man diese Daten auf der Festplatte speichert und vor deren Weitergabe nicht sicher löscht.

Stellenangebot **Call-Center-Agent/in** ***Arbeitsamt 14-04-2004***

Sehr geehrte Damen und Herren,

hiermit bewerbe ich mich um eine Vollzeit-Anstellung als Call Center-Agent in Ihrem Unternehmen. Ich habe bereits in dieser Sparte, insbesondere auch im Outbound gearbeitet und bin innerbetrieblich im Umgang mit Kunden geschult worden. Mein letztes Arbeitsverhältnis endete zum 31.08.2003, somit wäre ich ab sofort verfügbar.

Über eine Einladung zu einem persönlichen Gespräch würde ich mich sehr freuen.

Meinen Werdegang entnehmen Sie bitte den beiliegenden Unterlagen.

Abbildung 3: Auszug aus einem Bewerbungsschreiben (Speichermedium: Festplatte)

So geschehen in den vorliegenden Fällen, von denen wir exemplarisch drei herausgegriffen haben. Wir fanden den Lebenslauf eines 27-jährigen Süddeutschen, der 1996 den Hauptschulabschluss erworben hat. Bemerkenswert ist der Hinweis, dass sein Vater unbekannt sei.

Interessant sind auch die Lebensumstände der 32-jährigen Referentin für Telekommunikation und Mediendesign, die sich in ihrer Freizeit gerne mit kreativem Gestalten, Aquarellmalerei und Schauspiel beschäftigt. Man erfährt auch gleich, dass sie ledig ist und keine Kinder hat.

Und dann ist da noch der 24-jährige Zerspanungsmechaniker aus Ostdeutschland, der angibt, seinen Grundwehrdienst noch nicht abgeleistet zu haben, und der seit zwei Jahren keinen Job mehr hat.

Alle diese Informationen, die sehr persönlich und privat sind, konnten wir ohne großen Aufwand den Festplatten entnehmen. Wir gehen davon aus, dass all diesen Personen und auch allen anderen, von denen wir Daten rekonstruieren konnten, gar nicht bewusst ist, welche Daten sie preisgeben. Sicherlich würden sie diese Lebensläufe niemals einfach so in den Abfall stecken, so dass jeder Nachbar sie aus der Mülltonne angeln könnte. Bei der Festplatte ist das noch viel einfacher und man bekommt sogar noch viel mehr Daten dazu geliefert.

Wenn das der Schützenverein erfährt …
Ein besonderes „Bonbon" fanden wir auf einer weiteren Festplatte. Wir rekonstruierten neben den persönlichen Daten des Vorbesitzers auch dessen E-Mail-Postfach und fan-

den darin diverse E-Mails. Dort waren neben Bestellungen bei einem Spezialladen für Fetisch-Gummiwaren auch Kontakte zu anderen Fetischliebhabern enthalten. Hier ein kurzer Auszug aus einer E-Mail, bei der es offensichtlich um die Bewertung einer Ferienwohnung hinsichtlich deren Tauglichkeit für SM-Praktiken ging.:

Fragen hätten wir da schon einige gehabt, aber die wurden durch die Fotos beantwortet, die auch auf der Festplatte gespeichert waren. Dort kann man zum Beispiel die Frau in ihrem Gummi-Outfit posieren sehen. Auf einem anderen Foto sieht man den Mann im Kreise seiner Freunde aus dem Schützenverein. Sicherlich sollen seine Kameraden nicht wissen, was er so in seiner Freizeit oder im Urlaub treibt …

Hallo ihr zwei

Wir sind Rubberpaar H. & H.

Wenn ihr mal wieder die Zeit habt, 3-4 Wochen am Stück fahren zu können, werden auch wir wieder dort hin fahren. Unsere Zeit dort haben wir sehr genossen und wo hat man schon die Möglichkeit seinen Sklaven ganz in Gummi und Kettenfesseln zu halten. Bei uns in der Mietwohnung ging es nicht, das klirren der Ketten wäre zu laut. Ausserdem ist ein schwimmen in Gummi oder bei ihm sogar in einem aufblasbaren Anzug, in unseren Hallenbädern auch nicht möglich.

Gruß H.

Ps.: Wenn ihr noch Fragen habt, Mailt uns einfach noch mal an

Abbildung 4: Auszug aus einer E-Mail (Speichermedium: Festplatte)

Diese Auflistung von privaten, persönlichen und geschäftlichen Daten könnte man noch beliebig fortführen. Man kann ganz klar erkennen, dass die Achtlosigkeit bei der Weitergabe von Datenträgern eines der größten Risiken für Missbrauch und Diebstahl von Daten ist. Hier helfen keine Firewall und kein Anti-Virus-Programm mehr. Die Daten werden in ihrer reinsten Form quasi auf dem Präsentierteller angeboten. Missbrauch ist damit Tür und Tor geöffnet!

Abbildung 5: Urlaubsfoto im Fetisch-Outfit (Speichermedium: Festplatte)

Blick in die USA

Erstmals haben wir auch Festplatten aus den Vereinigten Staaten in unsere Studie einbezogen. Dort wurde bereits im Januar 2003 von zwei Forschern des Massachusetts Institute of Technology eine Studie veröffentlicht, für die sie Festplatten bei eBay ersteigert und diese auf wiederherstellbare Daten untersucht haben. Das damalige Ergebnis der Studie war, dass der größte Teil der Festplatten noch Daten enthielt – von privaten bis hin zu Daten aus einem Geldautomaten einschließlich der Kontobewegungen der Bankkunden.[1] Hat sich in den Jahren etwas verändert? Wir wollten herausfinden, wie ausgeprägt die Sensibilität in dem Land mit dem größten IT-Markt im Vergleich mit der in Deutschland ist. Zu unserem Erstaunen stellten sich die Ergebnisse recht ähnlich zu denen aus Deutschland dar. Von den 80 in den USA erworbenen Festplatten waren lediglich 68 hardwaretechnisch intakt. Die 12 defekten Festplatten wurden nicht in die Studie einbezogen, was einer Quote von 17,6 % entspricht. Von 31 der intakten Festplatten konnten Daten rekonstruiert werden. Dies entspricht zwar „nur" einer Quote von knapp 45 %, jedoch standen uns lediglich 68 Datenträger zur Verfügung.

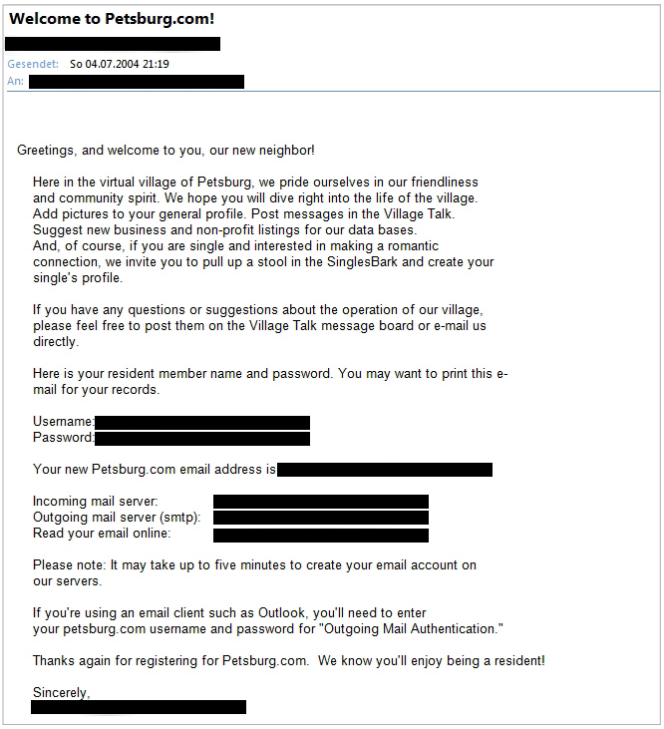
Auch auf den US-amerikanischen Festplatten konnten wir äußerst interessante Daten wiederherstellen. Hier standen neben den privaten Daten vor allem militärische Informationen im Vordergrund.

E-Mails

Neben privaten E-Mails fanden sich auch geschäftliche E-Mails auf den untersuchten Datenträgern. Insbesondere Zugangsdaten zu einem E-Mail-Account könnten für Unbefugte von Interesse sein, denn damit kann man nicht nur die E-Mails ohne Wissen des Postfachbesitzers lesen, sondern auch über dieses Postfach versenden. Im besten Fall ist es „nur" Spam, im schlimmsten Fall können damit auch Straftaten begangen werden (Stichwort „Phishing"). Und die Beweislast liegt dann beim Inhaber dieses Postfaches, der den Missbrauch möglicherweise gar nicht bemerkt und damit in das Fadenkreuz der Ermittler gerät.

Bewerbungsunterlagen aus einem Labor

Interessant war auch ein E-Mail-Archiv, in dem sich eine Reihe von Bewerbungen befand, die offensichtlich an ein Laboratorium für erneuerbare Energie in Colorado gerichtet waren. Alle Unterlagen waren vorhanden und dazu noch die Bewertung der Bewerber in einer Excel-Tabelle sortierbar nach Namen oder Punkten – sicherlich nicht unspannend für einen Mitbewerber, sich diese und andere Personalinformationen zu eigen zu machen.



Welcome to Petsburg.com!
[redacted]
Gesendet: So 04.07.2004 21:19
An: [redacted]

Greetings, and welcome to you, our new neighbor!

Here in the virtual village of Petsburg, we pride ourselves in our friendliness and community spirit. We hope you will dive right into the life of the village. Add pictures to your general profile. Post messages in the Village Talk. Suggest new business and non-profit listings for our data bases. And, of course, if you are single and interested in making a romantic connection, we invite you to pull up a stool in the SinglesBark and create your single's profile.

If you have any questions or suggestions about the operation of our village, please feel free to post them on the Village Talk message board or e-mail us directly.

Here is your resident member name and password. You may want to print this e-mail for your records.

Username: [redacted]
Password: [redacted]

Your new Petsburg.com email address is [redacted]

Incoming mail server: [redacted]
Outgoing mail server (smtp): [redacted]
Read your email online: [redacted]

Please note: It may take up to five minutes to create your email account on our servers.

If you're using an email client such as Outlook, you'll need to enter your petsburg.com username and password for "Outgoing Mail Authentication."

Thanks again for registering for Petsburg.com. We know you'll enjoy being a resident!

Sincerely,
[redacted]

Abbildung 6: Zugangsdaten zu einem E-Mail-Postfach (Speichermedium: Festplatte)

Bilder aus dem Irak

Viele US-amerikanische Soldaten bleiben mit ihren Familien in der Heimat via E-Mail und Internet verbunden. Daraus folgt, dass auch digitale Fotos verschickt werden. Auf sehr vielen Festplatten konnten wir solche Fotos rekonstruieren, was uns angesichts der geringen Anzahl von Festplatten, die wir in den USA erworben hatten, zunächst erstaunte. Betrachtet man aber die Anzahl der US-Soldaten im Irak, so haben vermutlich die meisten Amerikaner einen Angehörigen oder Bekannten in den Truppen, mit dem sie in Kontakt stehen.

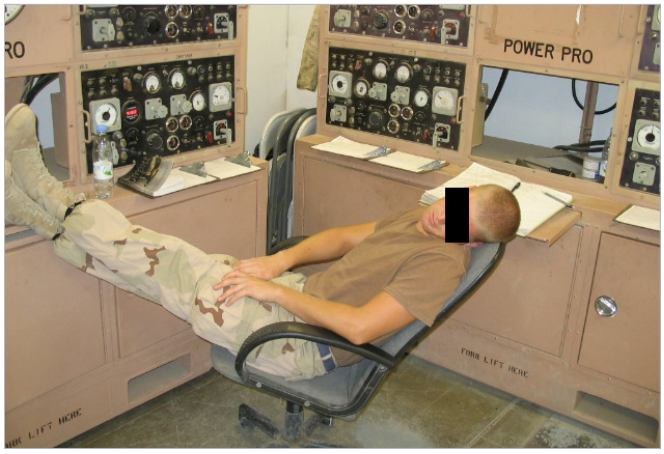


Abbildung 7: Pause im Irak (Speichermedium: Festplatte)

Abbildung 8: US-Soldat auf Flak-Geschütz (Speichermedium: Festplatte)

Abbildung 9: Freizeit im Irak (Speichermedium: Festplatte)

Abbildung 10: US-Soldat vor Armee-Jeep (Speichermedium: Festplatte)

Anti-Terror-Videos und Web-Zugangsdaten der US Air Force
Daran schließen sich nahtlos Videos an, die für die US Air Force entwickelt wurden und Anti-Terror-Trainings zeigen. Diese Informationen waren sicherlich nicht für Außenstehende gedacht.

Als Zugabe gab es auf dieser Festplatte auch gleich noch die vollständigen Daten für den Zugang zu einer Website der US Air Force, auf der man Informationen erhält, die als hochsensibel einzustufen sind. Selbstverständlich haben wir die Gültigkeit dieser Daten nicht überprüft, denn das ist strafbar. Es ist aber beängstigend, dass man so leicht an solche Informationen gelangen kann. Auch wenn dies vermutlich ein „Glückstreffer" ist – vor dem Hintergrund, dass wir nur 80 Festplatten in den USA erworben haben, beeindruckt es doch, dass auf so vielen Festplatten neben persönlichen Daten auch geschäftliche und militärische Geheimnisse zu finden waren.

Abbildung 11: Trainingsvideo für den Anti-Terror-Einsatz (Speichermedium: Festplatte)

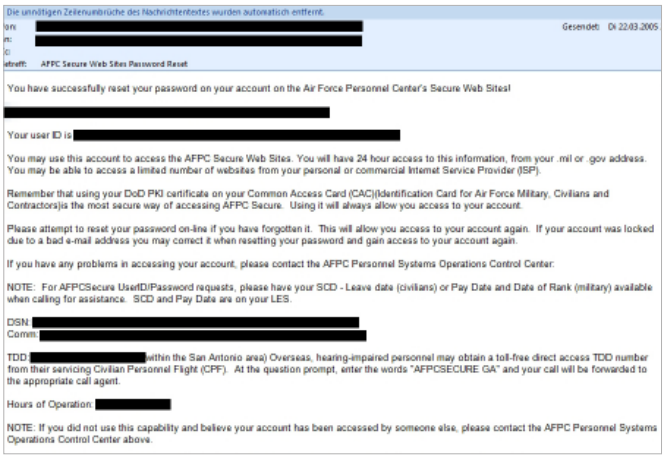


Abbildung 12: Zugangsdaten zu einer US-Militär-Website (Speichermedium: Festplatte)

Digitale Fotografie und USB-Sticks

Speicherkarten aus Digitalkameras
Digitale Kameras haben den klassischen Fotoapparaten mittlerweile den Rang abgelaufen. Immer mehr Fotos werden gemacht, immer mehr dieser digitalen Bilder werden gespeichert. Wir haben ja bereits gezeigt, wie viele dieser Fotos auf gebrauchten Festplatten zu finden waren. Deshalb wollten wir überprüfen, wie hoch die Wahrscheinlichkeit ist, diese Fotos auf den Speicherkarten selbst, die in den Kameras stecken, zu finden.

Die heutigen Digitalkameras verwenden in der großen Mehrzahl das FAT/FAT32-Dateisystem zur Speicherung der Daten, welches von Microsoft stammt und von Windows unterstützt wird. Sie sind also nichts anderes als sehr kleine Festplatten, die man über einen Kartenleser oder ein USB-Kabel mit seinem PC verbinden kann. Die Tatsache, dass ein Windows-Dateisystem verwendet wird, ermöglicht den direkten Zugriff auf diesen Datenträger, ohne dass aufwendige Zusatzsoftware notwendig wäre. Der Nachteil ist, dass diese Kameras auch genau nach dem gleichen Prinzip löschen. Trotzdem bieten viele Hersteller von Digitalkameras entsprechende Programme zur Bildbearbeitung und -übertragung an, um die Benutzung bequemer zu machen.

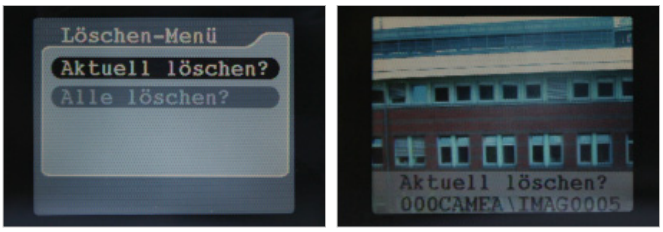


Abbildung 13/14: Der Löschdialog einer Digitalkamera

Beim Löschen erscheint genau wie bei Windows kein Hinweis, dass die Daten nicht für immer gelöscht werden. Auch hier können die Fotos mit einer Datenrettungssoftware sehr einfach rekonstruiert werden.
(Speichermedium: Digitalkamera)

Vor diesem technischen Hintergrund konnten wir die Datenrekonstruktion mit derselben Software durchführen, die wir bereits bei den Festplatten eingesetzt hatten. Da wir anders als bei einer normalen Festplatte einen homogenen Datenbestand erwarten konnten (eine Digitalkamera speichert die Bilder immer in demselben Dateiformat), konnten wir die Suche noch entsprechend optimieren. Auf diesen Speicherkarten haben wir dann circa 3100 Fotos gefunden, die insgesamt einem Datenvolumen von 1,8 GByte entsprachen. Unter diesen Bildern waren fast ausschließlich private Fotos von einzelnen Personen und Familien, teilweise auch deren Autos. Einige Bilder waren ausgesprochen intim. Da wurden schon mal Fotos mit dem Selbstauslöser in erotischen Situationen geschossen. Insgesamt wurde sehr deutlich, dass diese Fotografien nicht für andere bestimmt waren – zumindest nehmen wir das an.

Abbildung 15: Digitale Urlaubsbilder (Speichermedium: Speicherkarte)

Abbildung 16: Fotos von der Digitalkamera eines Meerschweinchen- und Kaninchenzüchter (Speichermedium: Speicherkarte)

USB-Sticks
Wie bei den Speicherkarten aus Digitalkameras verhält es sich auch bei USB-Sticks. Diese haben mittlerweile ebenfalls sehr große Kapazitäten erreicht, so dass sie häufig als Back-up-Medium eingesetzt werden. Und genau wie bei Festplatten führt das Löschen von Dateien oder das Formatieren von USB-Sticks nicht zum endgültigen Entfernen der Daten. Bei unseren Analysen fanden wir auf den 12 USB-Sticks verschiedene Daten, so unter anderem die Steuererklärung einer Heilpraktikerin oder Klausuren einschließlich deren Lösung im Fach Personalwirtschaft von einer Berufsschule.

Welche Ursachen hat diese Unvorsichtigkeit?

Unwissenheit ist das Hauptproblem
Nach der Auswertung der vorliegenden Ergebnisse stellt sich die Frage, warum Benutzer ihre Datenträger nicht korrekt löschen, so dass die Daten nicht wiederherstellbar sind.

Viele sind sich sicherlich der Gefahr überhaupt nicht bewusst, denn sie glauben, dass das Löschen der Daten zu deren endgültiger Vernichtung führt. Das Papierkorb-Symbol von Windows entspricht aber dem Vorgang: Wenn Dateien mit dem Windows-Explorer gelöscht werden, dann kann man sie notfalls wieder aus dem Papierkorb herausholen. Leert man jedoch den Papierkorb, so suggeriert Windows durch einen Warnhinweis, dass die Dateien tatsächlich und unwiderruflich gelöscht werden.

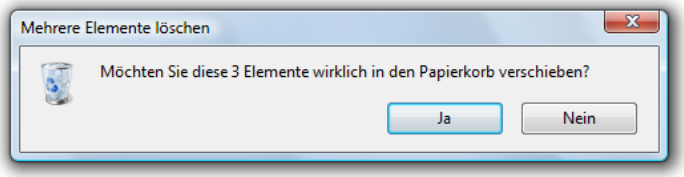


Abbildung 17: Die Warnung beim Verschieben von Dateien in den Papierkorb unter Windows Vista. Aus dem Papierkorb können die Daten wieder „herausgeholt“ werden.

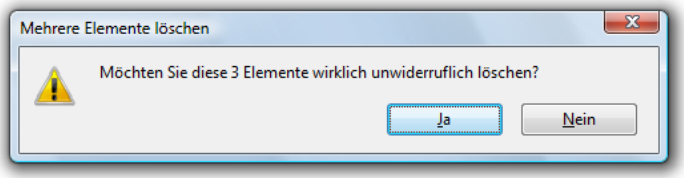


Abbildung 18: Die Warnung beim endgültigen Löschen der Dateien unter Windows suggeriert, dass die Daten wirklich gelöscht werden.

Auch in Firmen und Behörden scheint immer noch dringender Aufklärungsbedarf zu herrschen, denn auch in diesem Jahr haben wir wieder Daten gefunden, die so sicher nie in Umlauf gebracht werden sollten. Das sichere Löschen von Datenträgern ist in vielen Unternehmen hoffentlich als Standardprozedur etabliert, jedoch unterschätzen einige IT-Verantwortliche dieses Risiko noch oder es ist ihnen einfach nicht bewusst.

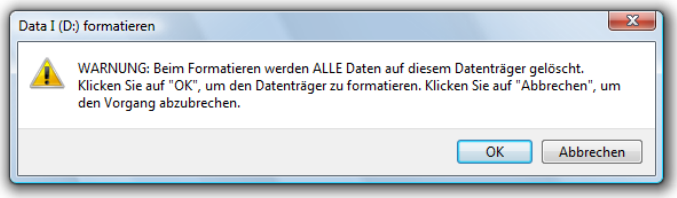


Abbildung 19: Auch beim Formatieren unter Windows wird dem Anwender mitgeteilt, dass die Daten gelöscht werden. Nach dem Formatieren sind diese unter Windows auch nicht mehr sichtbar, können aber mit Spezialsoftware schnell und einfach rekonstruiert werden.

Eine weitere Erklärung für die unbeabsichtigte Weitergabe persönlicher Daten hat sich während der Studie herausgestellt: Defekte Festplatten, die vom Benutzer nicht mehr benutzt werden können, weil Windows deren Erkennung verweigert, werden ausgemustert und durch neue ersetzt. Früher sind solche Platten vermutlich einfach in den Mülleimer gewandert, heutzutage finden sich bei eBay auch hierfür Käufer. Aber auch diesen Festplatten lassen sich mit ein wenig technischem Aufwand Geheimnisse entlocken, die der ursprüngliche Besitzer schon für immer verloren geglaubt hatte.

Ähnlich verhält es sich beim Formatieren der Festplatte. Der von Windows angezeigte Warnhinweis lässt den Benutzer in dem Glauben, dass nun alle auf der Festplattenpartition enthaltenen Daten für immer zerstört werden. Dies ist aber nicht der Fall. Windows schreibt lediglich den Bootsektor neu und erstellt ein neues „Hauptverzeichnis“. Alle anderen Daten bleiben nach wie vor erhalten und können leicht rekonstruiert werden.

Gefahr beim Gewährleistungsfall
Die Gefahr des Datenmissbrauchs lauert nicht nur beim Verkauf oder Verschenken alter Festplatten. Auch bei einer Reparatur gibt man in der Regel den gesamten Rechner ab – einschließlich der Festplatte. So können private Daten in falsche Hände gelangen. Deshalb ist es wichtig darauf zu achten, wem man seinen Rechner zur Reparatur anvertraut. Man sollte sich schriftlich zusichern lassen, dass die Daten weder gelesen noch kopiert werden, sofern dies nicht für die Durchführung des Reparaturauftrages notwendig ist.

Wer auf Nummer Sicher gehen möchte, baut die Festplatte vor der Abgabe beim Service aus. Dies ist jedoch nur möglich, wenn dadurch der Gewährleistungsanspruch nicht verloren geht und die Reparatur auch ohne Festplatte möglich ist.

Ignoranz
Letztendlich ist auch die Ignoranz nicht zu unterschätzen: Die Verkäufer wissen zwar von der Möglichkeit, dass der neue Besitzer Daten auslesen kann, schätzen diese Tatsache aber offensichtlich als eher unkritisch ein. Im Verlauf der Studie wurden drei Festplatten an uns übersendet, die vollkommen funktionstüchtig und sofort einsatzbereit waren. An dieser Stelle muss man sich fragen, ob solche Leute auch Ihre Dokumente in den Leitz-Ordnern lassen, wenn sie diese weitergeben. Hierbei handelt es sich um sträflichen Leichtsinn, denn selbst ohne Wiederherstellungssoftware können sämtliche Daten schnell und einfach ausgelesen werden.

Lösungen

Formatieren reicht nicht aus!
Bevor man geeignete Gegenmaßnahmen ergreifen kann, muss man zunächst wissen, woher die Gefahr des Wiederherstellens von Daten überhaupt rührt. Fest steht, dass das bloße Löschen oder Formatieren der Festplatte und anderer Speichermedien, wie es Windows oder auch Digitalkameras durchführen, definitiv nicht ausreicht, um die Daten endgültig zu löschen. Nur das wirkliche Vernichten der Daten durch die physikalische Zerstörung oder das sichere Überschreiben ist eine geeignete Maßnahme, um Datendiebstahl vorzubeugen. In den nachfolgenden Abschnitten werden diese beiden Verfahren kurz dargestellt.

Trügerische Sicherheit durch Verschlüsselung der Daten
Einer der elegantesten Wege zum Schutz der Daten ist deren Verschlüsselung. Dies bedeutet, dass bereits alle Daten auf der Festplatte verschlüsselt abgelegt werden. Nur durch Eingabe einer Benutzerkennung und zugehörigem Kennwort hat man Zugriff auf die Daten.

Microsoft hat seit Windows 2000 für diesen Zweck das Encrypted File System (kurz EFS, Verschlüsseltes Dateisystem) eingeführt. Sowohl in Windows XP als auch Windows Vista ist dieses aber erst aber der Professional bzw. Business Edition erhältlich. In Windows Vista Ultimate wurde die noch weitergehende Verschlüsselung „Bitlocker" integriert, die bereits vor dem Start des Betriebssystems aktiv wird und einen umfassenderen Schutz als EFS bietet.[2][3]

Auf alle vorgenannten Verfahren können Anwender der Home-Editionen nicht zugreifen, da sie in diesen Editionen nicht integriert sind. Sie müssen dazu zusätzliche Software erwerben und installieren. Dieser Installations- und Einrichtungsvorgang kann recht komplex sein, so dass viele darauf verzichten. Hinzu kommt, dass man bei vergessenem Kennwort keinen Zugriff mehr auf die Daten erhält. Und davor haben Benutzer mehr Angst als vor der Gefahr, dass die Daten später in falsche Hände geraten.

Der Vorteil der Verschlüsselung liegt darin, dass die Daten immer geschützt sind, also auch im Falle eines Diebstahls des Rechners. Auch muss der Benutzer sich nicht mehr großartig darum kümmern, denn das Betriebssystem übernimmt nach erfolgreicher Authentifizierung die gesamte Ver- und Entschlüsselung.

Der Nachteil einer Verschlüsselung in Bezug auf die Entsorgung ist die trügerische Sicherheit, in der man gewiegt wird. Die Behauptung, man müsse eine verschlüsselte Festplatte nicht mehr sicher löschen, ist schlicht falsch. Eine verschlüsselte Festplatte muss genauso sicher gelöscht werden wie jede andere unverschlüsselte Festplatte auch. Denn nur der Schutz durch ein Kennwort reicht nicht, um einen potenziellen Datendiebstahl zu verhindern. So kann ein Angreifer einfach versuchen, die Zugangsdaten durch einen gezielen Angriff zu ermitteln. Kennt der Angreifer sich mit dem Mechanismus der Verschlüsselung aus, so kann er noch gezielter nach den Daten auf der Festplatte suchen. Viele solcher Produkte legen ihre Schlüsselinformationen in bestimmten Sektoren ab, so dass man diese direkt ansteuern kann. Auch ist das Erraten von Benutzerkennung und Kennwort mit gewissen Kenntnissen des Vorbesitzers möglich, da viele Anwender simple Passwörter verwenden wie Namen ihrer Familienangehörigen oder Haustiere sowie Geburtstage. Besitzer verschlüsselter Datenträger, die auf Nummer Sicher gehen wollen, müssen daher eines der nachfolgenden Verfahren wählen.

Physikalische Zerstörung der Festplatte
Die physikalische Zerstörung der Festplatte ist eine der sichersten Methoden zur Vernichtung von Daten. Angefangen bei der Entmagnetisierung mit großen Elektromagneten bis hin zum Durchbohren und Häckseln der Festplatte gibt es verschiedene Methoden. Allen ist gemeinsam: die Festplatte ist nachher nicht mehr zu gebrauchen und kann nur noch als Sondermüll entsorgt werden. Das hat zum einen höhere Kosten zur Folge, zum anderen nicht unerheblichen – und im Heimwerker-Keller auch möglicherweise gesundheitsgefährdenden – Aufwand.

In vielen Firmen ist eine physikalische Zerstörung gar nicht möglich, da die Rechner einschließlich der Festplatten von Leasingfirmen stammen und sie nach Ablauf des Vertrages zurückgegeben werden müssen.

Sicheres Löschen von Daten mit Software
Die preiswerteste, unkomplizierteste und effektivste Methode zum sicheren Löschen von Daten ist die Softwarelösung. Es gibt eine Reihe spezieller Programme auf dem Markt, die das sichere Löschen von Daten ermöglichen. Hierbei werden spezielle Verfahren verwendet, die beispielsweise vom US-amerikanischen Verteidigungsministerium (Department of Defense, DoD) und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen werden.[4][5]

Einer der bekanntesten Algorithmen ist der erweiterte NISPOM (US DoD 5220.22-M ECE), der ein siebenmaliges Überschreiben definiert. Hierbei werden abwechselnd Zufallswerte, vordefinierte Werte und deren Komplement geschrieben. Aus heutiger Sicht gilt die von Peter Gutmann

entwickelte Methode zum sicheren Löschen als verlässlichste, bei der die Daten bis zu 35 Mal überschrieben werden. Eine softwaretechnische Rekonstruktion der Daten wird durch dieses Verfahren unmöglich gemacht.[6]

Die O&O Software GmbH bietet für diesen Zweck das Programm O&O SafeErase an, das ein sicheres Löschen aller Daten gewährleistet. Es ist sogar in der Lage, einen gesamten Rechner einschließlich der Systemdateien zu löschen, so dass mit wenigen Klicks ein Rechner sicher gesäubert werden kann, bevor er weitergegeben wird. O&O SafeErase bietet fünf verschiedene Modi zur Datenlöschung, unter anderem die zuvor beschriebenen Verfahren.

Fazit

Zusammenfassung und Vergleich mit den Ergebnissen aus den vorherigen Jahren.
Wir haben das Thema Datenschutz und Datensicherheit bereits in den Jahren 2004 und 2005 in Studien behandelt und herausgefunden, dass die meisten Anwender sich auf das normale Löschen durch das Betriebssystem verlassen. Diese Studie zeigt, dass sich leider wenig geändert hat und die Mehrheit der Windows-Benutzer ihre Daten immer noch sorglos aus der Hand gibt. [7] [8]

Erstmals haben wir in dieser Studie nicht nur Festplatten aus Deutschland, sondern auch aus den USA analysiert. Dabei stellte sich heraus, dass in den USA das sichere Löschen von Daten offensichtlich verbreiteter ist als in Deutschland.

Sicherlich können wir aufgrund der geringen Anzahl an erworbenen Festplatten keine generelle Aussage treffen; wir vermuten aber, dass das US-amerikanische Gesetz, das Unternehmen zur Datenlöschung verpflichtet, dazu geführt hat, dass zumindest Unternehmen dies viel konsequenter einhalten als beispielsweise Unternehmen in Deutschland.

Auch die Ergebnisse bezüglich der Speicherkarten aus Digitalkameras und USB-Sticks waren erschreckend. Drei Viertel der Datenträger waren nicht sicher gelöscht, so dass die Daten rekonstruiert werden konnten. Insgesamt ist zu bemerken, dass die Anzahl digitaler Fotos in den vergangenen drei Jahren rapide zugenommen, was mit der Verbreitung von Digitalkameras erklärt werden kann.

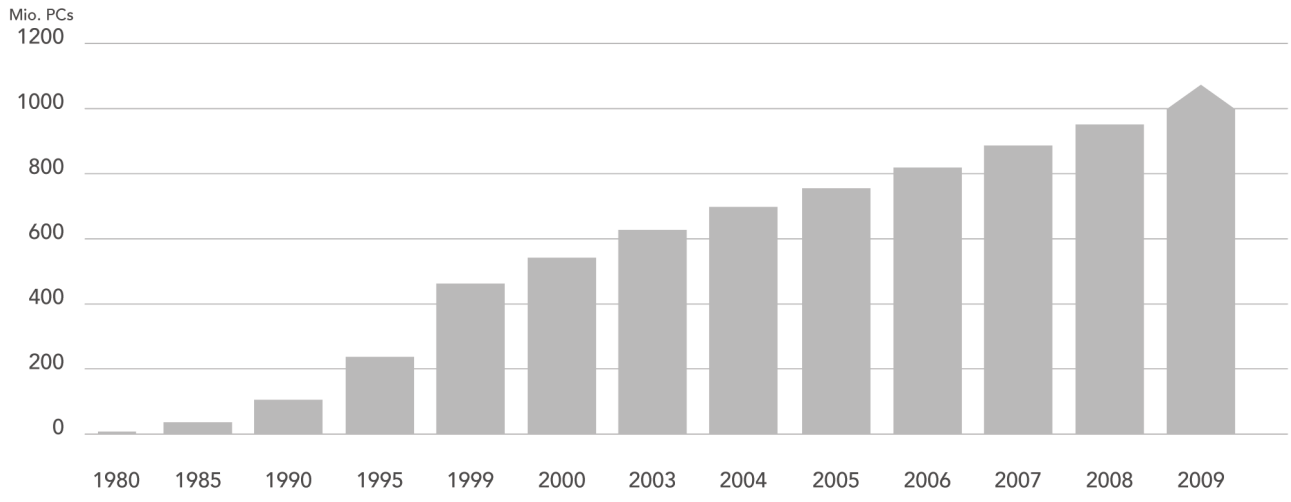
Die Entwicklung bei den Datenfunden über die Jahre betrachtet gibt keinen Anlass zur Entwarnung. Immer noch wird die große Mehrzahl der Datenträger als vermeintlich gelöscht betrachtet und sorglos weitergegeben. Ob mit solchen Daten bereits gezielt Missbrauch getrieben wird, bleibt im Dunkeln. Wichtig ist es, die PC-Anwender permanent auf diese Gefahr aufmerksam zu machen. Anstrebenswert ist ein ähnliches Problembewusstsein, wie es beim Thema Angriffe aus dem Internet bei der großen Mehrheit bereits besteht. Zurzeit ist das Thema der Datenrekonstruktion von alten Speichermedien immer noch wenig populär, was aus unserer Sicht einen entscheidenden Fehler darstellt.

Gefahr des Datenmissbrauchs
Wenn jemand fremde Zugangsdaten missbraucht, dann kann er damit sogar die Identität der ahnungslosen Person annehmen. Er kann in ihrem Namen im Internet einkaufen, Dinge ersteigern oder E-Mails schreiben. Das kann verheerende Konsequenzen haben, zumal der Geschädigte nachweisen muss, dass die Bestellungen und E-Mails nicht von ihm selbst stammen. Das kostet Zeit, Geld und kann zusätzlich eine Menge Unannehmlichkeiten bedeuten.

Abbildung 20: Wiederherstellungsquote von funktionsfähigen Festplatten

Ergebnisse erzeugt mit Datenrettungsprodukten der O&O Software GmbH

Abbildung 21: Anzahl installierter PC Systeme weltweit [9][10]



Bei sorgloser Weitergabe von Datenträgern in Firmen und Behörden muss die Geschäftsleitung handeln, denn bei Versäumnissen im Bereich Datenschutz ist sie in der Haftung gegenüber den Betroffenen und den Anteilseignern. Schadenersatzansprüche und peinliche Publizität der verlorenen Daten können schnell eine existenzielle Gefahr für das Unternehmen darstellen.

Was bei privaten Daten vielleicht einfach nur ärgerlich ist, kann bei geschäftlichen Daten den Ruin bedeuten. Eine Veröffentlichung interner Daten kann zivil- und sogar strafrechtliche Konsequenzen haben. Personenbezogene Daten mit Einzelheiten über Auftraggeber und Auftragnehmer haben wir auch in diesem Jahr wieder gefunden. Würden diese Daten an die Öffentlichkeit gelangen, wäre dies das Aus für die betroffenen Betriebe, denn ihre Reputation wäre unwiderruflich zerstört. Ein breites Betätigungsfeld für alle möglichen Personen – nicht nur für Mitbewerber.

Vertrauen ist gut, Kontrolle ist besser!
Für den normalen PC-Anwender ist die physische Zerstörung der Festplatte aus mehreren Gründen kein gangbarer Weg: Er müsste erheblichen Aufwand betreiben, um die Festplatte unbrauchbar zu machen und hätte dann noch das Problem der Abfallentsorgung, denn Festplatten dürfen als Elektronikschrott nicht im Hausmüll entsorgt werden. Darüber hinaus würde er den Erlös, den er beim Verkauf der Festplatte erzielen würde, verlieren.

Das Löschen mit einer Spezialsoftware wie O&O SafeErase ist kostengünstig, einfach und absolut sicher. Wer kontrollieren möchte, ob die Daten wirklich gelöscht wurden, kann dies mit Datenrettungsprogrammen wie O&O DiskRecovery überprüfen. Es werden keine Daten mehr wiederherstellbar sein. Für welche Möglichkeit man sich auch entscheidet, zu bedenken ist immer, dass das einfache Löschen mit Windows oder der Digitalkamera niemals ausreichend ist!

Abbildung 22: Dialog von O&O SafeErase 3 zum sicheren Löschen von Daten

Speichern und Löschen von Daten auf Festplatten

Wie werden Daten gespeichert?
Bevor man Daten endgültig löschen kann, muss man zunächst wissen, wo sich diese Daten überhaupt befinden, denn oft ist es nicht nur die eigentliche Datei, die gelöscht werden muss.

Beim Kopieren, Verschieben und Komprimieren von Dateien bleibt die ursprüngliche Version der Datei erhalten. Mit Vorsicht sind auch sogenannte Versionierungssysteme zu genießen, bei denen explizit alte Versionen von Dateien gespeichert werden, um sie später zum Beispiel für Vergleiche und Wiederherstellungen zu nutzen. Insbesondere ist an dieser Stelle auf das Windows-2003-Server-Betriebssystem mit seinen neuen Schattenkopien hinzuweisen. Diese sollen den Benutzer vor dem versehentlichen Ändern oder Löschen von Dateien auf dem Server bewahren. Deshalb werden Änderungen an den Dateien in speziellen Speicherbereichen der Festplatte aufbewahrt, um so alte Versionen wiederherstellen zu können. Insofern ist das Löschen dieser (Schatten-(Dateien notwendig, um die Daten vollständig zu vernichten.

Aber auch Windows selbst erstellt Kopien der Daten: Temporäre Dateien enthalten Zwischenversionen der eigentlichen Datei und in der Auslagerungsdatei werden Speicherbereiche, die nicht mehr in den Hauptspeicher passen, aufbewahrt, um später wieder in den Hauptspeicher geladen zu werden. Temporäre Dateien werden zwar in der Regel beim Beenden des zugehörigen Programms gelöscht, aber auch hier ist das Löschen wieder nur das Freigeben des Speicherplatzes auf der Festplatte, so dass sich auch diese Daten rekonstruieren lassen.

Versteckte Datenspeicher
Daten verbergen sich aber auch noch an einigen anderen Stellen, auf die man als Benutzer normalerweise keinen Zugriff hat. Eines dieser Probleme stellen die sogenannten Cluster Tips dar. Jede Festplatte wird beim Formatieren in Zuordnungseinheiten (Blöcke) unterteilt. Sie sind die kleinsten Einheiten einer Festplatte, die von dem Betriebssystem verwendet werden können. Bei den heutigen Größen von Festplatten im zweistelligen Gigabyte-Bereich sind Zuordnungseinheiten mit einer Größe von 64 KByte keine Seltenheit mehr. Für das Betriebssystem bedeutet dies, dass, selbst wenn eine Datei nur 12 KByte groß ist, sie dennoch einen Speicherbereich von 64 KByte belegt. Der Rest dieses Blocks bleibt ungenutzt.

Normalerweise ist dies nicht problematisch, aber Speicherbereiche werden ja auch wieder freigegeben und mit anderen Daten überschrieben. Stellen wir uns nun vor, eine Datei hätte die Größe von 62 KByte und belegt damit einen Block. Diese Datei wird nun gelöscht, die Daten bleiben also erhalten, nur der Verzeichniseintrag verschwindet. In diesen Block wird nun eine neue Datei geschrieben. Ist diese Datei beispielsweise nur 10 KByte groß, werden auch nur die ersten 10 KByte des Blocks überschrieben, der Rest der alten Datei von immerhin 52 KByte bleibt erhalten. Dieses Beispiel lässt sich natürlich auf jede beliebige Datei übertragen, denn auch größere Dateien werden in Blöcke aufgeteilt, so dass der letzte Block in der Regel nicht vollständig belegt wird. Diese Datenfragmente werden als Cluster Tips bezeichnet. Das Problem hierbei ist, dass man an diese Fragmente nicht mehr herankommt, da der Block ja als zu einer existierenden Datei gehörig markiert ist. Nur mit Hilfe spezieller Löschprogramme können diese Bereiche gelöscht werden. Dieses Verfahren wird als Wiping (Verwischen) bezeichnet.

Daten „zwischen den Zeilen"
Das Speichern der Daten auf einer Festplatte erfolgt durch die Magnetisierung kleinster Eisenpartikel, die entsprechend ihrer Ausrichtung den Wert 0 oder 1 liefern. Diese Partikel sind auf der Oberfläche der Platten aufgetragen und werden in Spuren unterteilt, so dass der Kopf der Festplatte die Daten lesen und schreiben kann. Daten werden aber nicht nur in der Hauptspur der Festplatte, sondern auch in deren Ränder geschrieben, d. h. diese Nebenspuren enthalten ebenfalls die Daten. Normalerweise ist dies nicht problematisch, da die Festplatte beim Lesen dieses „Rauschen" herausfiltert. Für den potentiellen Angreifer sind diese Nebenspuren jedoch geeignet, die Daten wiederherzustellen. Früher wurden hierzu einfache Verfahren wie eine minimale Dejustierung der Festplattenköpfe verwendet. Heutzutage sind diese Nebenspuren aufgrund der höheren Speicherdichte schwieriger zu erreichen. Dafür sind ein erheblicher technischer und finanzieller Aufwand und sehr detailliertes Wissen notwendig, so dass vermutlich nur sehr gut ausgestattete Datenrettungsunternehmen oder Geheimdienste dazu in der Lage sind.

Löschen von Daten
Löschen ist nicht gleich Löschen. So löscht beispielsweise das Verschieben von Dateien in den Windows-Papierkorb und dessen anschließende Leerung die Daten nicht wirklich von der Festplatte. Vielmehr wird nur der Verzeichniseintrag entfernt, die eigentlichen Daten bleiben weiterhin auf der Festplatte und können somit rekonstruiert werden. Auch das Formatieren von Partitionen und selbst eine Low-Level-Formatierung auf BIOS-Ebene sind keine sichere Löschung, da die Daten – wenn auch mit mehr Aufwand – immer noch rekonstruiert werden können.

Ein- oder zweimaliges Überschreiben kann durch einen Fehlerfilter ausgeglichen werden und frühere Daten können wieder zum Vorschein gebracht werden. Dabei bedient man sich des physikalischen Effekts, dass die Nullen und Einsen auf der Festplatte durch analoge Signale dargestellt werden. Diese entsprechen aber nie vollständig einer 0 oder 1, sondern werden durch Verrauschen zu 0,05 beziehungsweise 1,05. Die Hardware gleicht diese Fehler durch Toleranzgrenzen aus, so dass eine 1 als 0,95 oder auch als 1,05 gespeichert sein kann. Aus diesen Schwankungen kann man mittels einer Mikroanalyse des analogen Datensignals und der Differenz zum zugehörigen Digitalsignal Rückschlüsse auf die vorherigen Datenwerte ziehen. Wird nämlich eine 0 durch eine 0 überschrieben, ergibt dies eine andere Feldstärke als wenn eine 0 durch eine 1 überschrieben wird. Dieses Verfahren ist zwar technisch aufwendig und auch nicht ganz billig, es zeigt aber, dass das bloße Überschreiben der Daten sie nicht auslöscht. Deshalb verwenden die gebräuchlichen Löschverfahren auch immer eine Kombination aus einem Datenwert und dessen Komplement, um das geschilderte Differenzverfahren unbrauchbar zu machen.

Impressum

Danksagungen
An dieser Stelle möchte ich mich bei meinen Kollegen Frank Witter, André Weiß und Matthias Günther für die Unterstützung bei der Durchführung der Studie bedanken. Sie haben nicht nur den wochenlangen Erwerb der Datenträger übernommen, sondern auch die Datenrekonstruktionen und Ermittlung der Statistiken.

Über den Autor
Diplom-Informatiker Olaf Kehrer ist Mitglied der Geschäftsleitung der Berliner O&O Software GmbH, die sich unter anderem mit den Themen sichere Datenlöschung und Datenwiederherstellung beschäftigt. Er ist mitverantwortlich für die Entwicklung neuer Technologien und Produkte auf dem Gebiet der Datensicherheit.

Hierzu zählen die Produkte O&O BlueCon, O&O DiskRecovery, O&O FormatRecovery, O&O UnErase sowie O&O SafeErase, die neben den in der Studie beschriebenen Löschverfahren auch die Wiederherstellung und Reparatur von Windows-Systemen ermöglichen.

Das Löschen mit einer Spezialsoftware wie O&O SafeErase ist kostengünstig, einfach und absolut sicher. Wer kontrollieren möchte, ob die Daten wirklich gelöscht wurden, kann dies mit Datenrettungsprogrammen wie O&O DiskRecovery überprüfen. Es werden keine Daten mehr wiederherstellbar sein. Für welche Möglichkeit man sich auch entscheidet, zu bedenken ist immer, dass das einfache Löschen mit Windows oder der Digitalkamera niemals ausreichend ist!

Über die O&O Software GmbH
Die O&O Software GmbH entwickelt seit 1997 Tools für Windows, die mittlerweile in mehr als 140 Ländern in verschiedenen Sprachen eingesetzt werden. Zu ihren Kunden zählen Privatpersonen, kleine und mittelständische Unternehmen, öffentliche Einrichtungen und internationale Konzerne. Das Produktportfolio umfasst Applikationen zur Performance-Optimierung, Datenwiederherstellung und sicheren Vernichtung von Daten. O&O-Produkte wurden in zahlreichen Vergleichstests als technologisch führend ausgezeichnet.

Weitere Informationen erhalten Sie im Internet oder direkt von uns:

O&O Software GmbH
Am Borsigturm 48
13507 Berlin
Deutschland

Tel +49 (0)30 4303 43-00
Fax +49 (0)30 4303 43-99
Web www.oo-software.com
E-Mail info@oo-software.com

Abbildungsverzeichnis

Literaturnachweis

1. Simson L. Garfinkel and Abhi Shelat, „Remembrance of Data Passed: A Study of Disk Sanitization Practices," IEEE Security & Privacy, vol. 1, no. 1, 2003, pp. 17-28.
2. Microsoft, „Encrypting File System for Windows Vista", Microsoft Inc., 2007; http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx
3. Microsoft, „BitLocker Drive Encryption", Microsoft Inc., 2007; http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx
4. Department of Defense, Department of Energy, Nuclear Regulatory Commission, Central Intelligence Agency, „National Industrial Security Program Operating Manual", 1995, 1997, 2001; http://www.dss.mil/isec/nispom.htm
5. Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch", BSI, 2006; http://www.bsi.bund.de/gshb/deutsch/
6. Peter Gutmann, „Secure Deletion of Data from Magnetic and Solid-State Memory", Usenix Assoc., 1996; http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
7. Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten", April 2004; http://www.oo-software.com/de/study/
8. Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten 2005", Mai 2005; http://www.oo-software.com/de/study/
9. Egil Juliussen, Ph. D., „Computers-In-Use Forecast", eTForecasts, Juni 2000; http://www.etforecasts.com/products/ES_cinuse.htm
10. Michael Kanellos, „A billion PC users on the way", CNET News.com, August 2004; http://news.com.com/A+billion+PC+users+on+the+way/2100-1003_3-5290988.html