O&O Software
www.oo-software.com

Deutschland Deine Daten

Studie zum Datenschutz bei gebrauchten Datenträgern

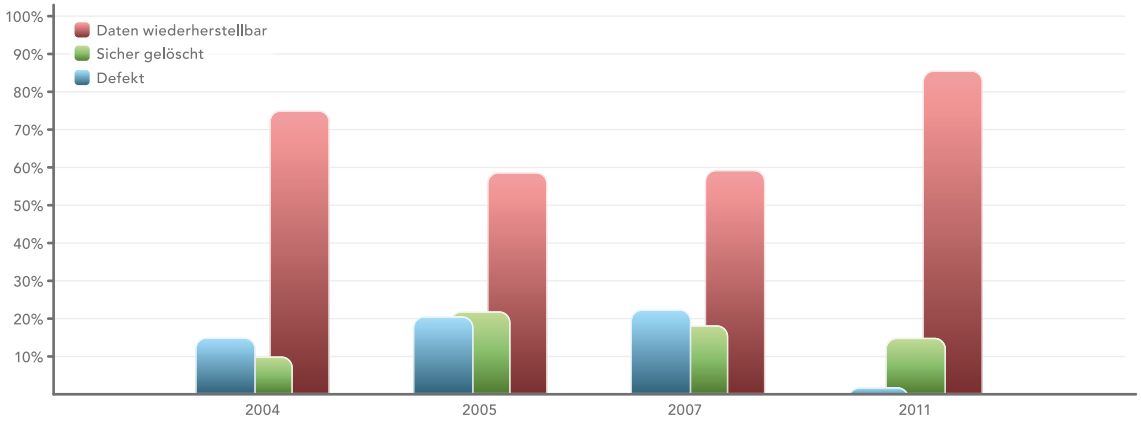
Dipl.-Inform. Olaf Kehrer • O&O Software GmbH, Berlin • August 2011

Einleitung

Unser Leben wird immer digitaler. Waren es vor ein paar Jahren nur Fotos und Videos, so ist es heute aufgrund der sozialen Netzwerke eine komplette Lebensspur, die wir im Internet hinterlassen. Wir verabreden uns über Facebook, wir twittern Neuigkeiten und wir geben über unser Mobiltelefon an, wo wir uns gerade aufhalten und ob es uns dort gefällt. Wir erzeugen immer mehr Daten, die wir bereitwillig auch immer mehr Leuten zur Verfügung stellen. Meist verschwimmt dort schon der Begriff von Freunden, Bekannten, Geschäftspartnern und eigentlich Unbekannten, mit denen wir unser Leben teilen. Macht man sich darüber mal Gedanken, dann werden sie auch schnell wieder verworfen. Argumente sind häufig, dass es entweder sowieso jeder macht oder dass sich schon keiner für seine persönlichen Daten interessieren wird.

Und genau dieser Irrglaube führt zu einer ansteigenden Verharmlosung der Datenfreizügigkeit gegenüber sich selbst und auch anderen. Immer wieder tauchen Berichte über die Nutzung von sozialen Netzwerken für die Beurteilung von Bewerbern auf[1]. Im Verborgenen sind auch unzählige Cyber-Kriminelle unterwegs, die solche Daten versuchen auszuwerten und zu missbrauchen. Illegale Quellen gibt es dafür mehr als genug und die großen Suchmaschinen helfen darüber hinaus auch fleißig bei der Beschaffung der Daten, denn es gibt immer mehr soziale Netzwerke, die durchsucht werden können.

Bereits vor sieben Jahren haben wir unsere Studie „Deutschland Deine Daten“ erstmals vorgestellt[2]. Damals wurden auf im Internet ersteigerten Festplatten sehr private und geschäftliche Daten gefunden, die leicht zu missbrauchen wären. Durch diese Studie und die öffentliche Berichterstattung wuchs das Bewusstsein der PC-Anwender, dass ihre Daten ausspioniert werden können und man dies nur mit dem sicheren Löschen von gebrauchten Datenträgern vermeiden kann. Über die folgenden Jahre war ein leichter Rückgang dieser Leichtsinnigkeit festzustellen.



Nach einer zwischenzeitlichen Zunahme der sicher gelöschten Datenträger haben diese nun ein Allzeit-Hoch erreicht

Nun aber zeigt die aktuelle Studie, dass im Jahr 2011 wieder weniger Leute wirklich ihre Daten sicher löschen. Mehr noch, es ist sogar ein Geschäftszweig entstanden, der mit diesen potenziellen Daten handelt. Im Folgenden werden diese Erkenntnisse vorgestellt und Maßnahmen beschrieben, wie man die versehentliche Weitergabe von privaten und geschäftlichen Daten erfolgreich verhindern kann. Nehmen wir also wieder Platz in deutschen Wohn- und Badezimmern.

Leichtsinnige Preisgabe auf alten Datenträgern

Über einen Zeitraum von drei Monaten wurden von der O&O Software GmbH verschiedene Datenträger erworben. Hauptsächlich wurden diese über einschlägige Verkaufsportale und Versteigerungsplattformen im Internet bezogen. Bei den Datenträgern handelte es sich neben den üblichen internen und externen Festplatten auch um solche, wie sie vorwiegend in sogenannten Fototanks (mobile Festplatten zum Anschluss an Digitalkameras) verwendet werden. Zusätzlich wurden auch Digitalkameras und Mobiltelefone mit den zugehörigen Speicherkarten erworben.

Anlieferung der Pakete mit den Datenträgern

Von den insgesamt 160 Datenträgern waren 137 und damit 85% nicht sicher gelöscht und enthielten Daten. 22 Datenträger waren sicher gelöscht, ein Datenträger war physikalisch defekt.

Auf diesen Datenträgern befanden sich über 53.000 Dateien im Format digitaler Fotos und über 4.500 Dateien im Format von Microsoft Word und Excel. Diese Dateien haben wir stichprobenartig gesichtet und fanden dabei neben zahllosen Fotos auch private Dokumente wie Lebensläufe oder Schriftverkehr mit dem Arbeitgeber. Wie auch bei den vorherigen Studien haben wir auch diesmal ausschließlich frei erhältliche Software zur Wiederherstellung der Daten verwendet[3], die von jedem PC-Anwender problemlos eingesetzt werden kann. Weder eine besondere Hardware noch eine Unterweisung in die Nutzung der Software sind hierfür notwendig.

Gefundene Daten

Urlaubs- und Familienfotos sind erwartungsgemäß die häufigsten Dateien, die auf privaten Datenträgern zu finden sind. Aber auch Dokumente wie Bewerbungsschreiben, Lebensläufe oder Urkunden sind dabei gewesen. Diese Datenfunde sind auch naheliegend, dient doch der PC heutzutage nicht nur als „Schreibmaschinenersatz" für Bewerbungen und das Anfertigen von Kopien von Zeugnissen. Er dient auch als Datenspeicher für die digitalen Bilder. Ist die Speicherkarte voll, werden die Bilder übertragen und dauerhaft gespeichert. Gelöscht wird nur sehr selten etwas. Und sicher gelöscht wird schon gar nichts.

FKK-Urlaub

Auf einem Datenträger fanden wir gleich eine ganze Reihe von Aktfotos aus dem FKK-Urlaub. Als Beispiel nur ein Foto der harmloseren Natur. Betrachtet man diese Bilder im Kontext des Urlaubs und der Ersteller, dann handelt es sich um recht harmlose und „normale" Aufnahmen. Landen diese aber in den falschen Händen und im Internet, kann dies extrem peinliche und unangenehme Folgen haben.

Toiletten-Bilder statt Klo-Sprüchen

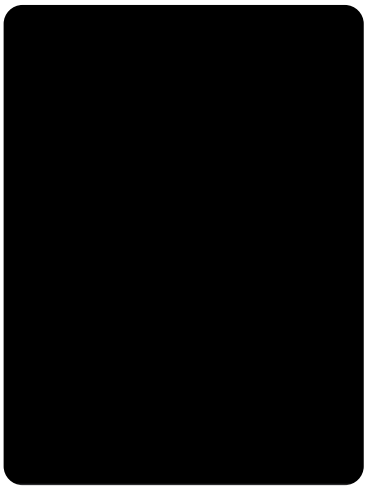
Waren früher noch Sprüche an der Klo-Tür modern, so scheinen es heute Toiletten-Fotos zu sein. Auf unzähligen Datenträgern haben wir in der Vergangenheit immer wieder Portraits und „Selbstbildnisse" auf der Toilette gefunden. Und die Häufigkeit dieser Fotos nimmt zu. Mittlerweile machen nicht nur Männer solche Fotos, sondern auch Damen haben uns mit einem gewissen artistischen Geschick entsprechende „Einblicke" präsentiert.

Mittendrin statt nur dabei

Stichwort „tiefe“ Einblicke: das Fotografieren der eigenen Körperöffnungen scheint mittlerweile ein Hobby der Deutschen geworden zu sein. Noch nie zuvor hatten wir so viele verschiedene Materialien auf unterschiedlichen Datenträgern aus allen Teilen Deutschlands vorliegen. Das nachfolgende Bild einer Dame war das Highlight. Der Balken auf dem Foto verdeckt die wesentlichen Teile. Mehr können wir leider nicht zeigen.

FKK am Strand

Von wegen ungestörtes Örtchen



Mittendrin statt nur dabei - das ist kein Fehler, das Bild soll schwarz sein!

Urkundenfälschung und Identitätsdiebstahl

Das folgende Beispiel zeigt rein exemplarisch, wie leicht sich Dokumente elektronisch manipulieren lassen. Wir fanden eine Original-Urkunde mit Abschluss zur Immobilienmaklerin. Diese haben wir kurzerhand auf Angela Merkel ausgestellt. Und diese Fälschung ist noch nicht einmal perfekt, sondern in wenigen Minuten mit Windows Paint erstellt worden.


URKUNDE

[redacted]

Geprüften
Immobilienmaklerin-IMI

IMI
IMMOBILIEN-INSTITUT

Original-Urkunde (persönliche Daten geschwärzt)


URKUNDE

Angela Merkel

Geprüften
Immobilienmaklerin-IMI

IMI
IMMOBILIEN-INSTITUT

Gefälschte Urkunde

Ganz persönlich

Wir haben aber nicht nur sehr eindeutige Fotos gefunden, sondern auch die ganz normalen Alltagsfotos, die auf Partys oder zuhause gemacht werden. Sicherlich kann man jetzt darüber streiten, ob diese wirklich so privat sind, weil sie heutzutage sowieso jeder bei Facebook & Co. einstellt. Aber genau das ist der Punkt: der Ersteller des Fotos entscheidet, ob, wie und wann ein solches Foto in den sozialen Netzwerken auftaucht oder auch nicht. Verliert man jedoch die Kontrolle über solche Bilder, dann können andere damit machen, was sie wollen. Auch wenn man eine rechtliche Handhabe dagegen haben mag, so ist die Durchsetzung doch recht aufwändig. Und sind die Fotos einmal im Internet im Umlauf, ist es nahezu unmöglich, diese jemals wieder zu löschen. Es existieren einfach zu viele Orte, an denen sie gespeichert werden können.

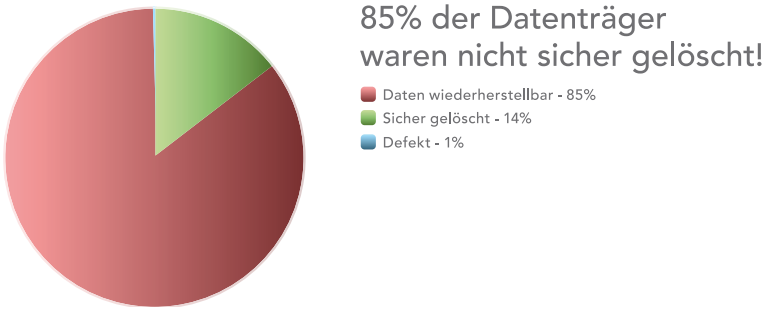
Junge Dame mit zwei Eiern im Mund

Kleine Katze beim Katerfrühstück?!

Welche Gründe führen zur leichtsinnigen Preisgabe persönlicher Daten?

Keine Veränderung des Benutzerverhaltens gegenüber früher

In unseren früheren Studien aus den Jahren 2004 bis 2007[2,4,5] beobachteten wir immer wieder ein leichtsinniges Verhalten der Besitzer von Datenträgern bei deren Weitergabe an Fremde. Zwischenzeitlich konnten wir eine geringfügige Abnahme der wiederherstellbaren Datenträger feststellen. In der aktuellen Studie hat diese jedoch wieder signifikant zugenommen. Eine mögliche Erklärung könnte das zurückgegangene Bewusstsein dieser Problematik oder auch eine „neue Freizügigkeit" mit den eigenen Daten durch die sozialen Netzwerke sein.

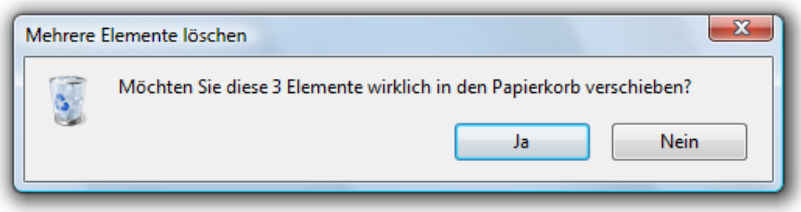


Nur jeder sechste Datenträger wird vom Vorbesitzer sicher gelöscht.
Alle anderen geben mehr oder weniger freiwillig sensible Daten preis.

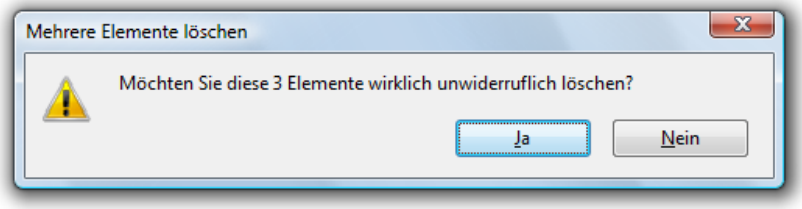
Im Ergebnis werden immer noch persönliche und teilweise sehr private Daten, aber auch geschäftliche Informationen, leichtfertig weitergegeben. Und auch hier ist wieder die alte Ursache der Grund: das einfache Löschen oder Formatieren von Datenträgern vernichtet die Daten nicht sicher, so dass sie schnell und einfach wiederhergestellt werden können.

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. Mit dem Papierkorb-Symbol von Windows verhält es sich jedoch folgendermaßen: Wenn man Dateien mit dem Windows-Explorer löscht, also in den Papierkorb verschiebt, kann man sie ebenso wieder aus dem Papierkorb herausholen. Leert man jedoch den Papierkorb, suggeriert Windows durch einen Warnhinweis, dass die Dateien tatsächlich und unwiderruflich gelöscht werden.



Die Warnung beim Verschieben von Dateien in den Papierkorb unter Windows. Aus dem Papierkorb können die Daten ganz einfach wieder hergestellt werden.



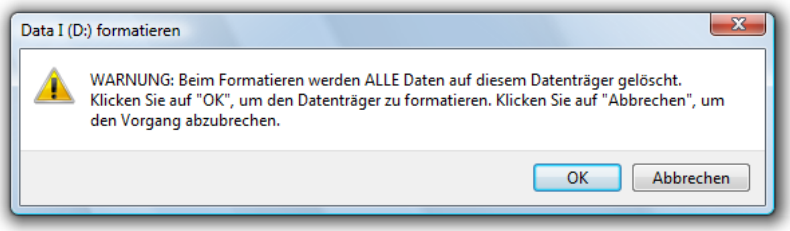
Die Warnung beim endgültigen Löschen der Dateien unter Windows suggeriert, dass die Daten wirklich gelöscht werden.

Defekte Datenträger sind nicht immer defekt

Defekte Datenträger, die nicht mehr benutzt werden können, weil Windows deren Erkennung verweigert, werden ausgemustert und durch neue ersetzt. Früher sind diese vermutlich einfach entsorgt worden, heutzutage finden sich online auch hierfür Käufer. Aber auch diesen Datenträgern lassen sich mit geringem technischen Aufwand Geheimnisse entlocken, die der ursprüngliche Besitzer schon für immer verloren geglaubt hatte.

Formatieren löscht nicht die Daten

Ähnlich verhält es sich beim Formatieren der Datenträger. Der von Windows angezeigte Warnhinweis lässt den Benutzer in dem Glauben, dass nun alle enthaltenen Daten für immer zerstört werden. Dies ist aber nicht der Fall. Windows schreibt lediglich den Startsektor neu und erstellt ein neues (leeres) Inhaltsverzeichnis. Alle anderen Daten bleiben nach wie vor erhalten und können leicht rekonstruiert werden. Stellen Sie sich hierfür einfach ein Buch vor, dessen Inhaltsverzeichnis man herausreißt, die Kapitel und Seiten aber drin lässt. Ganz leicht können Sie so mit dem Durchblättern der Seiten das Inhaltsverzeichnis wieder rekonstruieren. Genau nach diesem Prinzip macht das auch eine Datenrettungssoftware.



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.

Mit der Einführung von Windows Vista hat Microsoft an dem Algorithmus zum Formatieren etwas geändert: es werden nun Nullen in die Sektoren geschrieben, um die darin enthaltenen Daten zu löschen. Doch dies alleine löst nicht die beschriebenen Probleme. Zum einen handelt es sich hierbei um kein sicheres Verfahren zum Löschen, denn es existieren Methoden, um auch diese Daten wieder zu rekonstruieren. Zum anderen kann Windows selbst nicht die Systempartition formatieren, weil sich ja darauf die Dateien für das Betriebssystem befinden. Hierfür kann nur eine Spezialsoftware wie O&O SafeErase[6] eingesetzt werden. Und zu guter Letzt: die Standardeinstellung beim Formatieren unter Windows ist die Schnellformatierung, die keine Daten löscht, sondern nur das Inhaltsverzeichnis neu schreibt.

Komplettrechner - Vorsicht beim Gewährleistungsfall

Die Gefahr des Datenmissbrauchs lauert nicht nur beim Verkauf oder Verschenken alter Datenträger. Auch bei einer Reparatur oder einem Umtausch gibt man in der Regel den gesamten Rechner ab – einschließlich der Festplatte. So können private und auch geschäftliche 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.

Faulheit und Ignoranz
Schließlich bleibt noch eine spezielle Anwendergruppe: sie sind einfach zu faul oder ignorant, um bei der Herausgabe nicht sicher gelöschter Daten ein mögliches Problem zu sehen. Nach dem Motto „Das interessiert sowieso keinen" oder „Das ist ja so unwahrscheinlich" wird dann leichtsinnig alles weitergegeben.

Im Verlauf der Studie wurden 13 Datenträger an uns übersendet, die vollkommen funktionstüchtig und sofort auszulesen waren. Man muss 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 konnten sämtliche Daten schnell und einfach ausgelesen werden.

Das Leben wird immer digitaler

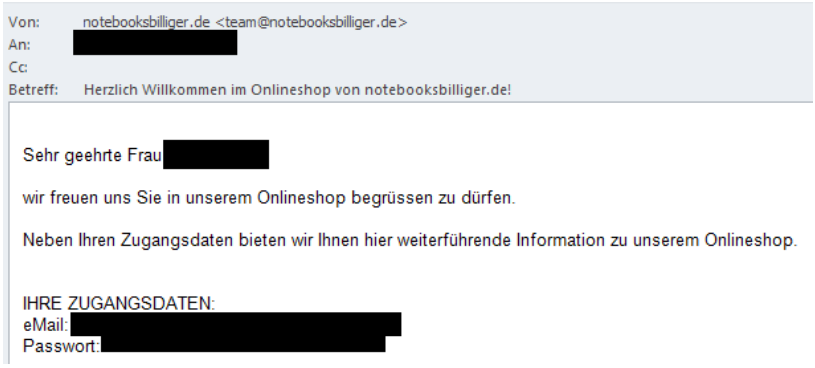
In den vergangenen Jahren hat sich das Leben im Internet nahezu vollständig gewandelt: hat man früher noch Fotos privat gespeichert und eventuell für Abzüge ins Fotolabor gebracht oder auch mit Freunden und Bekannten über USB-Stick oder per E-Mail ausgetauscht, so werden heute Fotos mit Handys gemacht und praktisch sofort ins Internet geladen. Auf Seiten wie Facebook und Flickr werden täglich über 5 Millionen neuer Bilder hochgeladen, Tendenz steigend[7]. Und meistens bleiben sie dort auch für immer. Das Thema Privatsphäre wird zwar häufig diskutiert[8], aber letztendlich tut dies den sozialen Netzwerken keinen Abbruch: täglich kommen neue Nutzer hinzu, die bereitwillig ihre Daten nicht nur dem Unternehmen, sondern auch allen Freunden, Bekannten und unbekannten Dritten preisgeben. Der vermeintliche Vorteil aus dieser Preisgabe scheint einen höheren Wert als die potenziellen Gefahren zu haben. Doch diese lauern nicht nur im Netz, sondern auch auf den lokalen Datenträgern, wenn diese achtlos entsorgt oder weitergegeben werden.

Durch die Verbreitung von Fotos, Videos, persönlichen Daten und Nachrichten in sozialen Netzwerken entsteht eine neue Gefahr: man selbst verliert die Kontrolle über die eigenen Daten. Wenn Freunde bei Facebook das eigene Profil aufrufen und Fotos anschauen, werden diese auf deren Rechnern im sogenannten Browser-Cache abgelegt. Dieser dient normalerweise zur Beschleunigung des Surfens im Internet. Er behält aber auch die Daten, wenn die Seite von Facebook längst wieder geschlossen ist. Und zwar so lange, bis diese Daten sicher gelöscht wurden. Dies geschieht so gut wie nie. Zwar werden ältere Daten nach Ablauf bestimmter Zeiten oder dem Überschreiten einer gewissen Datenmenge gelöscht. Aber dieses Löschen ist wie üblich bei Windows kein wirkliches Löschen: lediglich die Einträge im Inhaltsverzeichnis der Festplatte werden entfernt, die Daten bleiben jedoch erhalten und können mit einer Datenrettungssoftware auf Knopfdruck wiederhergestellt werden.

Dies bedeutet, dass man nicht nur selbst auf das sichere Löschen seiner Daten achten muss, sondern dass auch alle Freunde und Bekannte, an die man solche Daten schickt oder die über die eigenen Profilseiten in sozialen Netzwerken surfen, dies tun müssten. Genau wie bei einer Hochzeit, wenn viele Leute Fotos machen und jeder diese dann privat bei sich speichert. Nur dass durch die blitzschnelle Verbreitung und Vernetzung der heutigen Zeit die Daten überall sein können.

Missbrauchsmöglichkeiten der Daten

Die Zeiten, in denen massenhaft Schadsoftware an möglichst viele Empfänger gesendet wurde, sind vorbei. Heutzutage werden gezielt Personen angegriffen, die Zugriff auf vertrauliche oder wertvolle Informationen haben[9]. Diese werden von kriminellen Computer-Hackern zuvor genau ausgespäht und ihre Gewohnheiten analysiert. Dateien von alten Datenträgern sind da ein wahres Festmahl. Unbefugte erhalten damit nicht nur Zugriff auf persönliche Daten wie Fotos, Videos und Musik, sondern erlangen auch Informationen über E-Mail- und Surf-Verhalten, Zugriff auf die Namen von Freunden, Kollegen und Geschäftspartnern. Mit diesen Informationen können Cyber-Kriminelle eine Schadsoftware in eine E-Mail verpacken, die von einem vertrauten Absender mit einem bekannten Thema stammt. Schauen sich diese Computer-Hacker dann noch die alte Systemkonfiguration an, können sie sogar Rückschlüsse ziehen, welches Mailprogramm und welche Schutzsoftware verwendet wird, um Lücken in diesen gezielt auszunutzen. Im schlimmsten Fall wird der oder die Betroffene den Angriff nicht mal merken, bis es zu spät ist. Dann schon können Kontodaten oder auch Zugangsdaten zu lohnenden Datenquellen entwendet und missbraucht sein.


Von: notebooksbilliger.de <team@notebooksbilliger.de>
An: [redacted]
Cc:
Betreff: Herzlich Willkommen im Onlineshop von notebooksbilliger.de!

Sehr geehrte Frau [redacted]

wir freuen uns Sie in unserem Onlineshop begrüssen zu dürfen.

Neben Ihren Zugangsdaten bieten wir Ihnen hier weiterführende Information zu unserem Onlineshop.

IHRE ZUGANGSDATEN:
eMail: [redacted]
Passwort: [redacted]

Zugangsdaten zu einem Online-Einkaufsportal für Notebooks

Natürlich gibt es auch noch die „klassischen" Missbrauchsvarianten wie das Ausspähen von Kennwörtern für Online-Portale, die gerne auch in unverschlüsselten Dateien gespeichert werden. Oder die sehr intimen Fotos, die dann auch mal „zurückverkauft" werden oder in „Amateurforen" landen. Über den Missbrauch von harmlosen Kinderfotos im Sommerurlaub am Strand oder im Badezimmer mag man gar nicht mehr nachdenken. Es gibt viele Varianten, wie solche Daten mehr oder weniger heimlich missbraucht werden und großen Schaden anrichten können.

Neues Geschäftsfeld

Bei unseren Testkäufen im Internet sind wir zufällig auch auf ein neues Geschäftsfeld gestoßen: der Handel mit Datenträgern, bei denen der Verkäufer suggeriert, dass noch Daten vorhanden sein könnten. Dazu werden gerne Formulierungen wie „wurde nur privat genutzt" oder „müsste eigentlich leer sein" verwendet, die andeuten sollen, dass noch Daten rekonstruierbar sind. Wir haben einige dieser - vollkommen überteuerten - Datenträger zu Testzwecken erworben. Und siehe da: sie sind alle vollkommen sauber und sicher gelöscht. Es lässt sich auch erkennen, dass hier mit einer professionellen Software gearbeitet wurde, so dass der Verkäufer ganz klar nur den „unsicheren PC-Anwender" gibt, um einen möglichst hohen Preis für den Datenträger zu erzielen.

Der Käufer kann sich nicht mal beschweren, da er wohl kaum die versehentliche Herausgabe von Daten des Verkäufers einfordern kann. Ein interessantes Spiel mit der Neugierde der Käufer, aber dennoch ein fragwürdiges „Geschäftsmodell".

Verkaufsanzeige bei eBay für einen USB-Stick - schön auf einer Damenunterhose fotografiert, um den Käufer noch mehr „anzuspornen"

Hinweis im Text, dass der Stick „eigentlich leer sein müsste"

Möglichkeiten zum Schutz vor ungewolltem Datenverlust

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 einfache Löschen oder Formatieren der Festplatte und anderer Speichermedien, wie es Windows oder auch Digitalkameras durchführen, 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 Verfahren kurz dargestellt.

Festplatte - Trügerische Sicherheit durch Verschlüsselung der Daten
Einer der elegantesten Wege zum Schutz der Daten ist deren Verschlüsselung. Dies bedeutet, dass bereits alle Daten auf einer Festplatte verschlüsselt abgelegt werden. Nur durch eine erfolgreiche Authentifizierung erhält man Zugriff auf die Daten. Microsoft hat mit Windows 2000 für diesen Zweck das Encrypted File System (kurz EFS, Verschlüsseltes Dateisystem) eingeführt. Sowohl in Windows XP als auch Windows Vista war dieses aber erst ab der Professional bzw. Business Edition enthalten. In Windows Vista Ultimate wurde die noch weitergehende Verschlüsselung „Bitlocker“[10,11] integriert, die bereits vor dem Start des Betriebssystems aktiv wird und einen umfassenderen Schutz als EFS bietet.

Auf alle vorgenannten Verfahren können Anwender der Home-Editionen nicht zugreifen, da sie in diesen Editionen nicht integriert sind. Sie müssen dazu entweder die teureren Windows-Versionen oder 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 häufig 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. Der Benutzer muss sich nicht mehr großartig um die Sicherheit der Daten sorgen, denn das Betriebssystem übernimmt die gesamte Ver- und Entschlüsselung. Der Nachteil einer Verschlüsselung in Bezug auf die Entsorgung ist die trügerische Sicherheit, in der der Anwender 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 versierter Hacker einfach versuchen, die Zugangsdaten durch einen gezielten Angriff zu ermitteln. Kennt er 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 Bereichen der Festplatte 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 sehr einfache Passwörter verwenden wie Namen ihrer Familienangehörigen oder Haustiere sowie Geburtstage[12]. Besitzer verschlüsselter Datenträger, die auf Nummer Sicher gehen, müssen daher auch eines der nachfolgenden Verfahren wählen.

Physikalische Zerstörung der Datenträger

Die physikalische Zerstörung der Datenträger ist eine der sichersten Methoden zur Vernichtung von Daten. Angefangen bei der Entmagnetisierung mit großen Elektromagneten bis hin zum Durchbohren und Häckseln der Datenträger gibt es verschiedene Methoden. Allen ist gemeinsam: der Datenträger 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 der Datenträger gar nicht möglich, da zum Beispiel die Arbeitsplatzrechner einschließlich der Festplatten von Leasingfirmen stammen und sie nach Ablauf des Vertrages zurückgegeben werden müssen.

Sicheres Löschen von Daten mit spezieller Software

Die preiswerteste, unkomplizierteste und effektivste Methode zum sicheren Löschen von Daten ist der Einsatz einer speziellen Anwendung. Es gibt eine Reihe spezieller Programme auf dem Markt, die das sichere Löschen von Daten ermöglichen. Hierbei werden spezielle Verfahren verwendet, die unter anderem vom US-amerikanischen Verteidigungsministerium[13] und vom Bundesamt für Sicherheit in der Informationstechnik (BSI)[14] empfohlen werden.

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.[15]

Die O&O Software GmbH bietet für diesen Zweck das Programm O&O SafeErase[6] an, das ein sicheres Löschen aller Daten gewährleistet. Es ist sogar in der Lage, einen gesamten Rechner einschließlich der Systemdateien zu löschen (sog. TotalErase-Funktionalität[16]), so dass mit wenigen Klicks ein Rechner automatisch und sicher gesäubert werden kann, bevor er weitergegeben wird. O&O SafeErase bietet sechs verschiedene Modi zur Datenlöschung, unter anderem die zuvor beschriebenen Verfahren.

Fazit

Die digitale Welt dreht sich immer schneller. Immer mehr Daten speichern wir selbst und werden über uns gespeichert. Und wir haben immer weniger Kontrolle darüber, wer wann wo darauf zugreifen kann. Umso wichtiger ist es, dass wir unsere ganz persönlichen, privaten Daten vor dem Zugriff von Fremden schützen. Gerade digitale Bilder, persönliche E-Mails, aber auch Bewerbungsunterlagen und Zugangsdaten für das Internet stellen ein erhebliches Potenzial für Missbrauch und finanziellen Schaden, im Falle von Unternehmen sogar möglicherweise den Ruin dar. Ein sorgloser Umgang mit diesen Daten muss daher in allen Phasen des (Daten-)Lebens vermieden werden.

Gerade die neue Popularität von sozialen Netzwerken, die ihre Mitglieder zum schnellen Hochladen von Fotos und Statusmeldungen geradezu animieren, senkt natürlich das Bewusstsein bei vielen Anwendern für die daraus entstehenden Gefahren. Vielen neuen Anwendern sind sie gar nicht bewusst, weil sie praktisch mit diesen Techniken aufwachsen. Diese sogenannten „Digital Natives“[17] haben ein ganz anderes Verständnis für ihre Daten. Sie teilen sie gerne mit ihren Freunden und Bekannten. Leider können aber die falschen Fotos von Parties auch Probleme bei Bewerbungen bei einem neuen Arbeitgeber erzeugen[1].

Computer-Hardware und auch immer mehr die sogenannten Smartphones haben eine nur noch kurze Lebensdauer. Diese ist mittlerweile nicht mehr durch den Ausfall der Hardware beschränkt, sondern zunehmend durch die Veröffentlichung neuer Produkte, die zum Kauf und damit zum Austausch der alten Geräte anregen. Diese alte Hardware wird dann verkauft oder verschenkt, ohne sich große Gedanken über den Verbleib der gespeicherten Daten zu machen. Ein einfaches Löschen reicht hier nicht aus, um Daten unwiederbringlich zu vernichten. Die vermeintlich gelöschten Daten können vom Nachbesitzer mit handelsüblichen Datenrettungsprogrammen wiederhergestellt und missbraucht werden. Unsere ausgeführten Beispiele waren nur exemplarisch und aufgrund der Datenmenge auch nur oberflächlich betrachtet. Man stelle sich nur vor, man würde noch mehr Zeit in eine solche „Datensichtung“ investieren, welche potenziellen Geheimnisse man noch zu Tage fördern könnte. Und das neu aufkommende Geschäftsfeld, dass mittlerweile Verkäufer von Festplatten explizit solche „Datenvoyeure“ mit entsprechenden Formulierungen im Angebot anlocken wollen, zeigt, dass hier schon ein entsprechender Markt existiert, der bislang von der Öffentlichkeit nicht wahrgenommen wird.

Die nächste Herausforderung für den Schutz von Daten stellt das momentan sehr populäre „Cloud Computing“ dar. Hierbei werden alle Daten auf Servern im Internet abgelegt. Der Anwender kann von jedem Punkt der Erde, an dem ein Internetzugang existiert, auf die Daten zugreifen. Diese schöne neue Welt des mobilen Anwenders hat aber auch seine Schattenseiten. Denn hier stellen sich die Fragen, wo - sprich in welchem Land - eigentlich die Daten gespeichert sind? Und wer hat

die Möglichkeit, darauf zuzugreifen? Gerade hat Microsoft zugeben müssen, dass auf die von ihren Kunden gespeicherten Daten US-amerikanische Ermittlungsbehörden zugreifen können, wenn sie das wünschen[18]. Und dabei spielt es keine Rolle, ob die Daten von einem US-Bürger oder einem Einwohner der EU dort gespeichert wurden. Hier zeigen sich insbesondere für Unternehmen die Gefahren für die Speicherung ihrer Daten in einer sogenannten „Public Cloud". So sehr der Anbieter es auch versichern mag, aber gegenüber staatlichen Institutionen hat man nur noch sehr selten eine Kontrollmöglichkeit, ob und wer darauf zugreifen kann.

Die zunehmende Nutzung der Cloud und auch sozialer Netzwerke wie LinkedIn, XING oder Facebook zum Austausch von Kontakten, Informationen und Daten birgt eine trügerische Sicherheit: denkt man, dass seine Daten dort sicher sind, weil sie ja lokal nicht mehr gespeichert sind, so muss einem bewusst sein: viele speichern ihre lokalen Anmeldeinformationen in ungeschützten Dateien oder sie speichern sie im Internet-Browser, damit sie nicht immer wieder eingegeben werden müssen. Außerdem existiert in der Regel von den Dateien, die man in die Cloud speichert, auch eine lokale Kopie, die auch ohne Zugriff auf die Cloud rekonstruiert werden kann.

Gelangt ein Angreifer an diese sensiblen Zugangsdaten, so kann er von jedem Ort der Erde auf diese Daten zugreifen und sie stehlen. War das früher auf die Daten auf dem Datenträger beschränkt, so kann man damit quasi sämtliche Daten bekommen. Und in der Regel wird der eigentliche Besitzer davon nicht mal etwas mitbekommen. Der Angriff ist sogar nicht nur auf die Vergangenheit beschränkt, sondern es können auch in Zukunft Daten abgegriffen werden, sofern die Anmeldeinformationen gleich bleiben.

Dieser und alle weiteren genannten Gründe stellen jeder für sich die Verpflichtung zum sicheren Löschen aller Datenträger dar, die man selbst nicht mehr benutzt. Egal, ob man sie verschenkt, verkauft oder einfach entsorgt. Jedem Besitzer muss bewusst sein, dass nicht sicher gelöschte Daten jederzeit und unkompliziert wiederherstellbar sind. Und dann genutzt werden können. Mit allen daraus entstehenden Konsequenzen.

Impressum

Danksagungen
An dieser Stelle möchte ich mich wie auch bei meinen vorherigen Studien bei meinen Kollegen für die Unterstützung bei der Durchführung der Studie bedanken. Sie haben nicht nur den Erwerb der Datenträger übernommen, sondern auch die Wiederherstellung der Daten und die Ermittlung der zugehörigen Statistiken.

Über den Autor

Olaf Kehrer ist Geschäftsführer der O&O Software GmbH und ist für die Produktentwicklung verantwortlich. Sein Fokus liegt auf der Entwicklung neuer Konzepte im Bereich Systemwerkzeuge und der Erweiterung und Fortführung existierender Produktlinien. Er hat die O&O Software GmbH im Jahre 1997 mitgegründet und hat selbst maßgeblich an der Entwicklung von O&O Produkten mitgewirkt. Auch heute ist er noch sehr nah am Puls der Entwicklung und verfolgt dabei immer das Ziel, die bestmöglichen Produkte für die Kunden zu realisieren. Darüber hinaus hat er auch die Studienreihe „Deutschland Deine Daten" verfasst, die den Umgang mit gebrauchten Festplatten und nicht gelöschten Daten analysiert. Olaf Kehrer hat an der Technischen Universität Berlin studiert und den Grad des Diplom-Informatikers erlangt.

Eingesetzte Software

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.

Über die O&O Software GmbH

Die O&O Software GmbH aus Berlin entwickelt und vertreibt seit 1997 Standardsoftware für Windows. Zu ihren Kunden zählen Privatpersonen sowie Unternehmen und öffentliche Einrichtungen. Die Produkte werden direkt und über ein Partnernetzwerk in mehr als 140 Ländern erfolgreich vertrieben. Das Produktportfolio umfasst Applikationen zur Performance-Optimierung, Datenwiederherstellung, sicheren Datenlöschung und Administration unter Windows. O&O Produkte wurden in zahlreichen Vergleichstests als technologisch führend ausgezeichnet. Weitere Informationen und kostenlose Testversionen aller Produkte sind auf der Website von O&O Software erhältlich.

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

Anhang: Funktionsweise der Datenspeicherung unter Windows

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-Server-Betriebssystem mit seinen 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 Terabyte-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 potenziellen 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 staatliche Organisationen 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 aufwändig 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.[5]

Literaturnachweis

- [1]Zeit Online, „Chefs prüfen Bewerber in sozialen Netzwerken", September 2009; http://www.zeit.de/online/2009/35/Firmen-Bewerber-Internet
- [2]Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten", April 2004; http://www.oo-software.com/de/study/study_ddd2004_de.pdf
- [3]O&O Software GmbH, „O&O DiskRecovery"; http://www.oo-software.com/oodiskrecovery/
- [4]Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten 2005", Mai 2005; http://www.oo-software.com/de/study/study_ddd2005_de.pdf
- [5]Olaf Kehrer, O&O Software GmbH, „Deutschland Deine Daten 2007", August 2007; http://www2.oo-software.com/press/ddd2007_de.pdf
- [6]O&O Software GmbH, „O&O SafeErase"; http://www.oo-software.com/oosafeerase/
- [7]Joshua Burton, „INFOGRAPHIC: How Much Daily Content Is Published To Twitter, Facebook, Flickr?", April 2011; http://www.scribbal.com/2011/04/infographic-how-much-daily-content-is-published-to-twitter-facebook-flickr/
- [8]Marc-Oliver von Riegen und Johannes Wagemann/DPA , „Nutzer meckern und Aigner ‚wirft mit Wattebällen'", April 2010; http://www.stern.de/digital/online/diskussion-um-facebook-nutzer-meckern-und-aigner-wirft-mit-wattebaellen-1556463.html
- [9]Andy Bloxham, The Telegraph, „Sony hack: private details of million people posted online", Juni 2011; http://www.telegraph.co.uk/technology/news/8553979/Sony-hack-private-details-of-million-people-posted-online.html
- [10]Microsoft, „Encrypting File System for Windows Vista", Microsoft Inc., 2007; http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfi lesystem.mspx
- [11]Microsoft, „BitLocker Drive Encryption", Microsoft Inc., 2007; http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx
- [12]Imperva, „Consumer Password Worst Practices", Juni 2010, http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf
- [13]U.S. Department of Defense, Defense Security Service, „National Industrial Security Program (NISP)", 2011; http://www.dss.mil/isp/fac_clear/download_nispom.html
- [14]Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch", BSI, Oktober 2009; http://www.bsi.bund.de/gshb/deutsch/

- [15]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
- [16]O&O Software GmbH, „O&O SafeErase Datenblatt“; http://www2.oo-software.com/datasheets/pdf/datasheet_oose5pro_de.pdf
- [17]Wikipedia, „Digital Native“; http://de.wikipedia.org/wiki/Digital_Native
- [18]Zack Whittaker, „Microsoft admits Patriot Act can access EU-based cloud data“, Juni 2011; http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based--cloud-data/11225