

Studie zum Datenschutz bei gebrauchten Festplatten

Deutschland Deine Daten

Dipl.-Inform. Olaf Kehrer

O&O Software GmbH, Berlin – April 2004



Nichts ist wichtiger als der Schutz von Daten vor unbefugtem Zugriff durch Fremde. Die meisten PC-Benutzer sind sich mittlerweile über die Gefahren durch Viren und Trojaner aufgrund der massiven Berichterstattung in den Medien bewusst. Aber wissen sie auch, dass gelöschte Daten von gebrauchten Festplatten mit handelsüblicher Software wiederhergestellt werden können und werden deshalb Daten sicher gelöscht? Die vorliegende Studie geht dieser Frage nach und kommt zu dem Schluss, dass sowohl deutsche Privatbenutzer wie auch Firmen mit ihren Daten fahrlässig unvorsichtig umgehen.

Im Jahre 2004 ist Deutschland auf dem Weg in das elektronische Kommunikationszeitalter. Immer mehr Briefverkehr wird per Email abgewickelt. Viele Deutsche verwalten Ihre Geldkonten nur noch online, weil es praktischer und preiswerter ist. Der elektronische Personalausweis und die elektronische Krankenakte werden von der Bundesregierung als nächster Schritt zu einem sicheren und zuverlässigen Datenaustausch zum Wohle der Bürger gepriesen. Bundeskanzler Schröder hat auf der Eröffnung der diesjährigen CeBIT dieses bereits für das Jahr 2006 angekündigt.

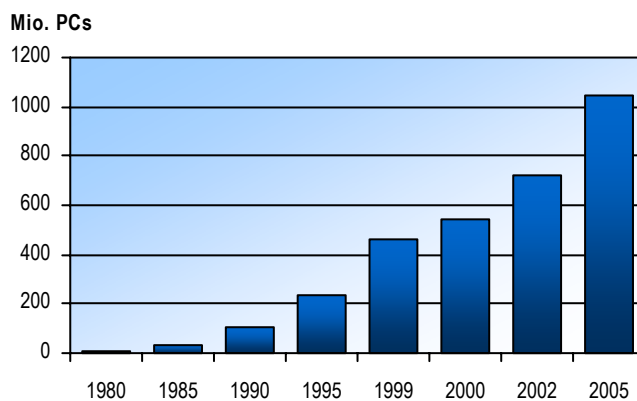
Eine der wichtigsten Aufgaben der heutigen Informationstechnik ist der Schutz von Daten gegen unberechtigte Zugriffe. Täglich nimmt die Zahl der Virusprogramme zu, die vom privaten Heimrechner bis hin zu Großrechenanlagen alles angreifen, was über das Internet erreichbar ist. Die meisten Benutzer schützen sich durch Anti-Virusprogramme, Firewalls und diverse andere Applikationen, die den Angriff auf den eigenen Rechner möglichst schwer machen sollen.

Dieses Bewusstsein wurde maßgeblich durch den Mitte 2000 in Umlauf gebrachten ILOVEYOU-Virus geprägt. Auch Microsoft hat in seinen neuen Betriebssystemen Windows XP und Windows Server 2003 die Sicherheitsmaßnahmen gegen

solche Virusattacken im Vergleich zu früheren Windows-Versionen erheblich verbessert. Es wurden diverse Schutzmechanismen vor Viren und Trojanern eingebaut, so dass auch Microsoft Outlook, der Quasi-Standard für Email-Programme, immer besser gegen Angriffe gewappnet ist.

Aber wie sieht es mit dem Schutz der eigenen Daten aus, wenn der Rechner veraltet oder defekt ist und ersetzt wird? Werden die Festplatten wirklich gelöscht, bevor der Rechner verkauft oder verschenkt wird? Wie sensibel gehen heutige PC-Benutzer mit diesem Thema um und wissen Sie überhaupt, wie leicht man Daten wiederherstellen kann?

Abbildung 1: Anzahl installierter PC-Systeme weltweit



Quelle: COMPUTERS-IN-USE FORECAST, eTForecasts[5]

Um diese Fragen zu klären, hat die Berliner O&O Software GmbH 100 Festplatten bei eBay ersteigert. Diese Datenträger wurden daraufhin untersucht, ob noch Daten enthalten sind und wie leicht es ist, sie wiederherzustellen.

Die eigentliche Gefahr

Sicher, jeder kennt die Gefahr durch böartige Virusprogramme, die den heimischen Rechner infizieren und möglicherweise persönliche Daten vor aller Welt preisgeben. Fast jeder hat diese Gefahr erkannt und durch immer mehr Gegenprogramme wird versucht, diese zu bannen. Deren fast tägliche Aktualisierung gehört mittlerweile schon zum PC-Alltag.

Doch gegen eine Gefahr scheint immer noch kein geeignetes Gegenmittel zu geben: den Leichtsinns des Benutzers. Und dieser insbesondere im Umgang mit den Daten, nachdem der zuvor so geliebte PC durch einen neuen ersetzt wird. Denn heutzutage wird ein PC nicht einfach weggeworfen – in vielen Fällen wird ihm eine ganz andere Ehre zuteil: die öffentliche Versteigerung bei eBay.

Jeder sollte wissen, dass man den Rechner vor der Abgabe an fremde Leute löscht. Man möchte ja nicht, dass die persönlichen Dokumente in die falschen Hände gelangen. Also wird die Festplatte formatiert und siehe da, anscheinend sind keine Daten mehr vorhanden. Das Betriebssystem ist verschwunden, der Rechner verweigert seine Arbeit gleich nach dem Starten. Also ist alles in bester Ordnung. Oder doch nicht?

Briefe und Dokumente, die wichtige oder persönliche Daten enthalten, wird wohl kaum jemand so einfach in den Papierkorb werfen. Man zerreit sie oder besser noch, man lässt die Dokumente von einem Aktenvernichter in Konfetti verwandeln. Der war früher nur in Unternehmen üblich, ist nun aber aufgrund des geringen Preises auch zunehmend in privaten Haushalten zu finden. Ist auch verständlich, denn wer möchte schon, dass der Nachbar in

der Mülltonne die eigenen Kontoauszüge, Liebesbriefe oder auch Kündigungsschreiben findet.

Mehr als 7,5 Millionen neue PC-Systeme in Deutschland in 2003

Laut eTForecasts sollen bis 2005 mehr als 1 Milliarde PC-Systeme weltweit im Einsatz sein (Abbildung 1). Laut Gartner Group und IDC wurden im vergangenen Jahr mehr als 150 Millionen neue PC-Systeme verkauft, davon alleine 7,5 Millionen Stück in Deutschland. Ein Großteil dieser Systeme hat alte PC-Systeme ersetzt. Diese alten PC-Systeme waren jedoch in vielen Fällen nicht defekt, sondern entsprachen lediglich nicht den heutigen Leistungsanforderungen. Die meisten wurden verkauft oder auch einfach verschenkt. Und hierbei handelt es sich nicht nur um private PC-Systeme, sondern auch sehr häufig um geschäftlich genutzte Rechner. Der Arbeitgeber ersetzt sie und verwertet die alten Geräte, um seine Kosten für die Neuanschaffung ein wenig zu senken. Häufig nimmt der Lieferant der neuen Rechner die alten in Zahlung oder „entsorgt“ sie einfach. Manchmal werden auch nur einfach die Rechner zerlegt und die wertvollsten Komponenten gewinnbringend einzeln verkauft. Diese finden nicht selten den Weg zu eBay, wo sie jeder zu einem mehr oder weniger günstigen Preis erwerben kann, um wiederum seinen Rechner aufzurüsten oder zu erweitern. So entsteht ein Kreislauf der PC-Komponenten, der in der Regel nur durch das hoffnungslose Veralten oder den Defekt einer solchen Komponente beendet wird.

Sensible Daten bei eBay zum Schnäppchenpreis

Doch wie verhält es sich mit dem Umgang mit Daten auf alten Festplatten und anderen Speichermedien bei deren Ausmusterung? Werden die Daten wirklich gelöscht oder vertraut der Benutzer darauf, dass ein Formatieren der Festplatte ausreicht?

Im Januar 2003 haben zwei Forscher des Massachusetts Institute of Technology eine Studie veröffent-



licht, in der sie Festplatten bei eBay ersteigert und diese auf wiederherstellbare Daten untersucht haben. Das Ergebnis der Studie war damals, dass der größte Teil der Festplatten noch Daten enthielt. Von privaten bis hin zu Daten aus einem Geldautomaten einschließlich der Kontobewegungen der Bankkunden.[7]

Hat sich aufgrund dieser Studie das Bewusstsein der PC-Benutzer verändert? Haben die Leute auf diese Ergebnisse nach mehr als einem Jahr reagiert?

Um dieser Problematik nachzugehen, hat die O&O Software GmbH im Verlaufe mehrerer Wochen Anfang 2004 Festplatten bei eBay ersteigert. Hierbei wurden die Festplatten willkürlich ausgewählt. Es wurden sowohl funktionstüchtige als auch defekte Festplatten erworben.

Diese Festplatten wurden mit Hilfe handelsüblicher Software auf wiederherstellbare Daten untersucht. Das Ergebnis: von 100 Festplatten waren nur zehn vollständig und sicher gelöscht. Alle anderen Festplatten enthielten Daten der Vorbesitzer – von illegaler Software über MP3-Musikdateien bis hin zu persönlichen Bankkontozugangsdaten und Liebesbriefen.

Patientendaten und Geschäftspapiere

Der Haupttreffer war eine Festplatte, die offensichtlich zuvor bei einer gesetzlichen Krankenkasse im Einsatz war. Sie enthielt nicht nur den internen Mailverkehr der Mitarbeiter, sondern auch Dienst-anweisungen zu Kostenübernahmen sowie den zugehörigen Schriftverkehr mit den behandelnden Ärzten – einschließlich der Patientendaten.

Diese Daten hätten es einem Unbefugten leicht ermöglicht, die Anschrift der Patienten zu ermitteln und mit diesen Informationen Missbrauch zu treiben – eine Unachtsamkeit, die sogar

juristische Konsequenzen haben kann.

Suche nach Gründen

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 auch deren endgültige Vernichtung bedeutet. So ist die Papierkorb-Metapher von Windows nicht von ungefähr. Wenn Dateien mit dem Windows-Explorer gelöscht werden, dann kann man sie notfalls wieder aus dem Papierkorb holen. Leert man den Papierkorb, so suggeriert einem Windows durch einen Warnhinweis, dass die Dateien tatsächlich und unwiderruflich gelöscht werden (Abbildung 2).

Ähnlich verhält es sich beim Formatieren der Festplatte. Der von Windows angezeigte Warnhinweis lässt den Benutzer im Glauben, dass nun alle auf der Festplattenpartition enthaltenen Daten für immer zerstört werden (Abbildung 3). 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.

Ein weiterer Grund hat sich während der Studie herausgestellt: Festplatten, die defekt sind und vom Benutzer nicht mehr benutzt werden können, weil Windows deren Erkennung verweigert. Diese

Abbildung 2: Das Leeren des Papierkorbs löscht die Daten nicht wirklich

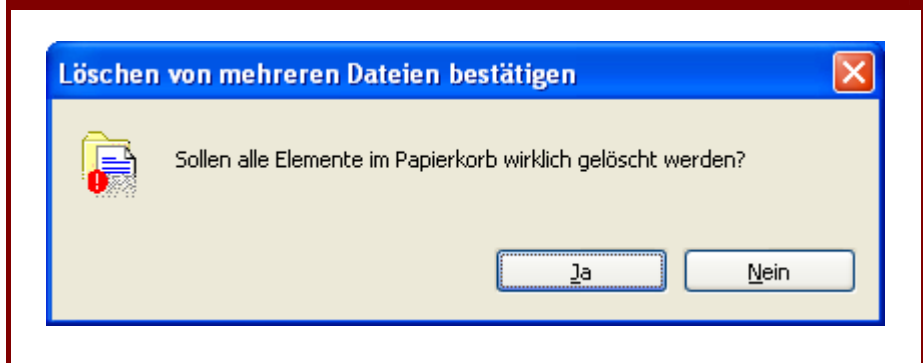
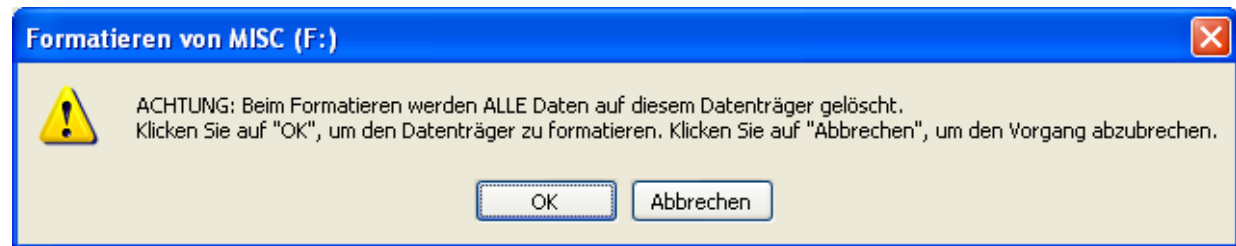


Abbildung 3: Der Warnhinweis vor dem Formatieren einer Festplatte ist irreführend



werden einfach ausgemustert und durch neue ersetzt. Früher sind solche Platten vermutlich einfach in den Mülleimer gewandert, heutzutage jedoch finden sich auf eBay auch hierfür Käufer. Aber auch von diesen Festplatten lassen sich mit ein wenig technischem Mehraufwand wieder Geheimnisse entlocken, die der ursprüngliche Besitzer schon für immer verloren geglaubt hatte.

Letztendlich ist auch die Ignoranz der gesamten Problematik nicht zu unterschätzen, d.h. die Verkäufer wissen zwar von der Möglichkeit, dass der neue Besitzer Daten auslesen kann, schätzen dies aber offensichtlich als eher unwichtig 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 verkaufen. Hierbei handelt es sich um sträflichen Leichtsinns, denn selbst ohne Wiederherstellungssoftware können sämtliche Daten schnell und einfach ausgelesen werden.

186 GByte Daten gefunden

Es wurden 100 Festplatten mit einer Gesamtkapazität von 526 GByte erworben. Hiervon waren 15 technisch defekt, so dass diese nicht weiter betrachtet wurden, da der Aufwand zur Wiederherstellung der Daten unverhältnismäßig groß gewesen wäre. Lediglich 10 Festplatten waren sicher gelöscht, alle anderen konnten entweder sofort oder nach einer

teilautomatisierten Wiederherstellung der Daten gelesen werden (Abbildung 5).

Insgesamt konnten über 590.000 Dateien mit einer Gesamtgröße von 186 GByte Daten rekonstruiert und gelesen werden. Hierunter befanden sich 15.248 Word-Dokumente und 3.918 Excel-Dateien. Weiterhin wurden 60 vollständige Outlook-Postfächer (PST-Dateien) gefunden, die entsprechenden Email-Verkehr enthielten.

Keine der Daten, die gefunden wurden, waren in irgendeiner Form verschlüsselt. Sie konnten einfach mittels Word, Excel oder Outlook geöffnet und gelesen werden.

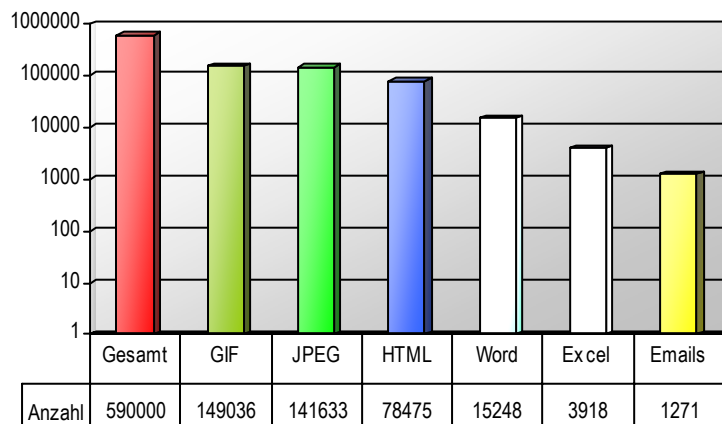
Im Wohnzimmerschrank deutscher PC-Benutzer

Die meisten Daten stammten von privaten Benutzern, die ihre persönlichen Dokumente, Bilder, Fotos und Emails gespeichert haben. Mit Hilfe einer der wiederhergestellten Festplatte wäre es möglich gewesen, eine komplette Fremdentität anzunehmen. Folgende Daten befanden sich auf ihr:

- Die eingescannte Unterschrift des Besitzers
- Bewerbungen und Lebensläufe
- Eingescannte Zeugnisse
- Der eingescannte Personalausweis sowie die eingescannte EC-Karte
- Bankvollmachten
- Internet- und Email-Zugangsdaten

Abbildung 4: Gefundene Dateitypen

Insgesamt konnten 590.000 Dateien wiederhergestellt werden. Hiervon entfiel der größte Teil auf Grafik- und Internetseiten (GIF, JPEG, HTML).
Über 15.000 Word- und fast 4.000 Excel-Dokumente waren lesbar. Hinzu kamen 60 Outlook-Postfächer (PST-Dateien) mit insgesamt 1271 Emails.
y-Achse der Tabelle ist logarithmisch aufgetragen



Ein anderer Benutzer hatte sogar den TAN-Brief der Bank eingescannt und abgespeichert, so dass es unter Umständen möglich gewesen wäre, Online-Transaktionen im Namen dieses Benutzers durchzuführen. Dies wurde jedoch von uns selbstverständlich nicht überprüft.

Weiterhin ließen sich folgende Daten wiederherstellen:

- Gerichtsurteile und Haftentlassungsbescheinigungen der Vorbesitzer
- Mehr als 10.000 MP3-Musikdateien, diverse Software-Raubkopien, Originallizenzen für Software usw.
- Private Emails in jeglicher Art und Weise
- Pornographisches Material jeglicher Art

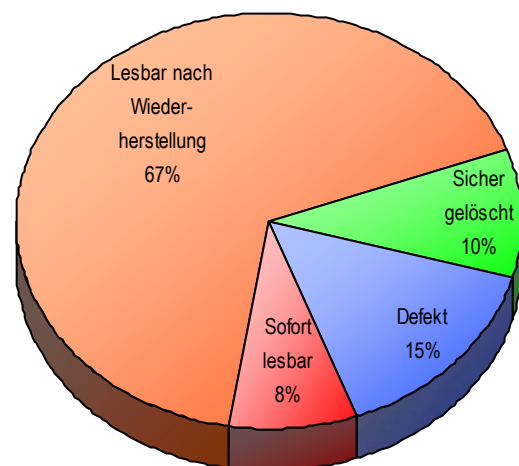
Zusammenfassend lässt sich feststellen, dass nicht nur äußerst private und sensible Informationen, sondern teilweise sogar strafrechtlich relevante Daten zu finden waren. Niemand würde eine fremde Person an seinen Wohnzimmerschrank lassen, um eingehend die darin aufbewahrten Aktenordner zu studieren. Aber diese Festplatten hatten die Qualität genau solcher Ordner.

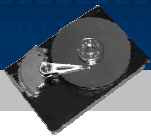
Festplatten einer Krankenkasse mit Patientendaten

Es ist leichtsinnig genug, dass private Benutzer ihre Daten achtlos – und leider auch unbewusst – weitergeben. Aber wesentlich dramatischer waren die Inhalte der Festplatten, die offensichtlich aus Unternehmen und Institutionen stammten.

Von einer großen gesetzlichen Krankenkasse erhielten wir die Festplatte eines Sachbearbeiters. Sie enthielt den vollständigen Schriftverkehr dieses Mitarbeiters – sowohl interne als auch externe Schreiben mit Ärzten einschließlich der zugehörigen

Abbildung 5: 75% der Festplatten waren lesbar





Patientendaten:

- Email-Archive, die sich öffnen und einsehen ließen
- Schreiben an behandelnde Ärzte über die Ablehnung von Kostenübernahmen einschließlich zugehöriger Patientendaten und Versicherungsnummer
- Interne Strategiepapiere und Arbeitsanweisungen, beispielsweise über die Höhe der Kassenbarbestände für die Geschäftsstelle
- Teile des Intranets als Offline-Kopie

Dieser Fall war die erste Festplatte, die uns erreichte. Aber dabei sollte es nicht bleiben: wenige Tage später erhielten wir von einem anderen Verkäufer eine weitere Festplatte genau dieser Krankenkasse – aus einer anderen Geschäftsstelle. Wiederum waren wichtige und sensitive Daten enthalten, u.a. die Verteilung von Leistungszulagen nach einem internen Schlüssel, der explizit als streng vertraulich gekennzeichnet wurde.

Bereits im Jahr 1997 hat John Markoff in der New York Times einen Artikel veröffentlicht, der von einem Fall berichtet, in dem eine Frau einen gebrauchten PC erworben hat, auf dem sie 2.000 Patientendaten einer Apotheke gefunden hatte.[3]

Offensichtlich scheint dieser Artikel wenig Gehör in Deutschland gefunden zu haben, obwohl – oder vielleicht gerade weil – er mittlerweile sieben Jahre zurück liegt.

Strategiepapiere und andere Unternehmensgeheimnisse

Die weiteren Festplatten aus Unternehmen enthielten eine Vielzahl vertraulicher und wichtiger, teilweise sogar strategischer, Daten, die mit Sicherheit in falschen Händen erheblichen Schaden erzeugen könnten.

So wurden Strategien beschrieben, wie die Schwächen eines bundesweiten Transportkonzerns ausge-

nutzt werden können, um daraus Vorteile zu gewinnen.

Interne Leistungszulagen, Kostenrechnungen, selbst Mitteilungen eines Vorstandsmitgliedes eines weltweiten Pharmakonzerns an seine Mitarbeiter über die Umsatzverteilung des vergangenen Geschäftsjahres und die Ziele für das kommende Jahr.

Auch von einer Agentur für Personalberatung (sog. Headhunter) waren Daten lesbar. Neben den Namen, Positionen und Anschriften der Zielpersonen in den entsprechenden Unternehmen, ihr Profil und der von den Auftraggebern gebotenen neuen Gehältern.

Die Liste ließe sich noch weiter führen. Es gab fast nichts, was nicht zu finden war. Selbst einen persönlichen Geschäftsbrief eines O&O Mitarbeiters der Partnerbetreuung an einen Interessenten konnten wir auf einer Festplatte wieder finden. Zumindest haben wir so erfahren, dass unsere Briefe auch ankommen.

Gegenmaßnahmen

Bevor man überhaupt geeignete Gegenmaßnahmen ergreifen kann, muss man zunächst wissen, woher die Gefahr des Wiederherstellens von Daten überhaupt rührt. In Anhang A ist eine ausführliche Beschreibung des technischen Hintergrundes gegeben, so dass wir an dieser Stelle nur zusammenfassend feststellen wollen, dass es grundsätzlich möglich ist, auch überschriebene Daten wiederherzustellen. Dies bedeutet zwar einen gewissen technischen Aufwand, aber für 1500-2000 Euro bekommt man bereits die geeignete Hardware einschließlich zugehöriger Software.

In den nachfolgenden Abschnitten sollen mögliche Verfahren zum Schutz vor Datenspiegung kurz dargestellt werden.

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 mit Windows 2000 für diesen Zweck das bestehende Dateisystem um EFS (Encrypted File System = Verschlüsseltes Dateisystem) erweitert.[4] In Windows XP ist dies leider nur in der Professional-Variante verfügbar, so dass alle Windows XP Home-Benutzer hiervon nicht profitieren können. Sie müssen zusätzliche Software erwerben und installieren. Dieser Installations- und Einrichtungsvorgang kann recht komplex sein, so dass viele darauf verzichten. Hinzu kommt, dass man bei vergessenen 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.

So können verschlüsselte Daten zwar auch wiederhergestellt werden wie alle anderen Daten, aber sie sind nicht zu gebrauchen, denn die Informationen sind nicht verwertbar. Benutzer, die auf Nummer Sicher gehen wollen, müssen eines der nachfolgenden Verfahren wählen.

Physikalische Zerstörung der Festplatte

Die physikalische Zerstörung der Festplatte ist eine der sichersten Methoden. Anfängen von der Entmagnetisierung mittels großer 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 beinhaltet zum einen höhere Kosten, zum anderen auch nicht unerheblichen –

und im Heimwerker-Keller auch möglicherweise gesundheitsgefährdenden – Aufwand.

In vielen Firmen ist eine physikalische Zerstörung gar nicht erst möglich, da die Rechner einschließlich der Festplatten von Leasingfirmen stammen, so dass deren Eigentum unverändert bei Ablauf des Vertrages zurückgegeben werden muss.

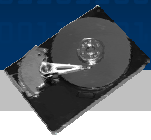
Software zum sicheren Löschen von Daten

Die preiswerteste, unkomplizierteste und effektivste Methode zum sicheren Löschen von Daten ist die Softwarelösung. Für diesen Zweck sind eine Reihe spezieller Löschroutinen 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) oder auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgeschlagen wurden.[1], [6]

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 sicherste, bei der die Daten bis zu 35 Mal überschrieben werden. Eine softwaretechnische Rekonstruktion der Daten wird bei diesem Verfahren unmöglich gemacht.[2]

Die O&O Software GmbH bietet für diesen Zweck zwei Produkte an: O&O BlueCon, das unter anderem das sichere Löschen gesamter Partitionen ermöglicht. Mit diesem Programm können selbst Systempartitionen gelöscht werden, was normalerweise bei laufendem System nicht möglich ist. Das zweite Produkt ist O&O SafeErase, das im Kontextmenü des Windows-Explorers integriert ist. So kann der Benutzer Dateien, Verzeichnisse und Partitionen sicher löschen. Bei beiden Programmen



stehen fünf verschiedene Modi zur Verfügung, unter anderem die zuvor beschriebenen Verfahren.

Fazit

Der Schutz von sensiblen Daten in Deutschland sowohl im Privat- als auch Unternehmensbereich ist zweigeteilt: so wird nahezu jeder einen Virensch scanner einsetzen, um Angriffe und Schäden von außen abzuwehren. Demgegenüber ist der Umgang mit den eigenen Daten nach der Entsorgung alter Festplatten als leichtsinnig und fahrlässig zu bezeichnen. Die dargestellten Erkenntnisse stellen nur einen kleinen Ausschnitt aus der Gesamtheit der täglichen Verkaufspraxis dar. Berücksichtigt man dies, so sind die gefundenen Daten auf nur 100 Festplatten ein deutlicher Hinweis, dass das Bewusstsein der PC-Benutzer im privaten wie im Unternehmensbereich noch sehr viel mehr geschärft werden muss.

Sicherlich kann man bei privaten Nutzern diese Unachtsamkeit auch zum Teil damit erklären, dass Windows ihnen suggeriert, sie würden mit der Formatierung der Festplatte alle Daten löschen. Dem professionellen Systemadministrator muss die Problematik jedoch bewusst sein, denn wer hat nicht schon die versehentlich gelöschten Daten eines Benutzers mittels Software wiederhergestellt. Insofern ist es ihre Pflicht, bei der Ausmusterung von PC-Systemen und Festplatten dafür zu sorgen, dass die zuvor gespeicherten Daten nicht in falsche Hände gelangen können. Alles andere ist gefährlich und fahrlässig.

Sensible Patientendaten

Das Beispiel der gesetzlichen Krankenkasse zeigt deutlich, dass in diesen Fällen bei der Verwertung der Datenträger unvorsichtig vorgegangen wurde. Wie sonst wäre es möglich gewesen, zwei Festplatten aus unterschiedlichen Geschäftsstellen von unterschiedlichen Verkäufern zu erhalten? Und wie hoch ist die Wahrscheinlichkeit bei nur 100 erworbenen Festplatten zwei von derselben Krankenkasse zu finden? Hier besteht dringender Bedarf der

Überprüfung der Vorgehensweise, denn Patientendaten zählen mit zu den sensibelsten Daten, die überhaupt existieren. Wer möchte schon, dass Teile seiner Krankengeschichte bei eBay erhältlich sind?

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. Man sollte deshalb darauf 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 weiterhin möglich ist.

Datenspeicher überall

Immer mehr Geräte beinhalten heutzutage Datenspeicher. Angefangen von PCs und Notebooks über Handys und PDAs (Elektronische Notizbücher im Pocketformat). Und alle Geräte lassen sich miteinander verbinden und synchronisieren, so dass persönliche Daten, Termine und Dokumente schnell auch dort zu finden sind, wo man es nicht vermuten würde.

Insbesondere Handys werden immer mächtiger. So verschmelzen momentan die elektronischen Notizbücher (PDAs) mit den mobilen Telefonen, um noch mehr Informationen ständig verfügbar zu machen. Handys werden normalerweise durch PIN-Codes gegen Missbrauch geschützt, so dass im Falle eines Verlustes zumindest der Zugriff auf die Daten nicht mehr möglich sein sollte. Sicherlich ist es nicht so leicht, Daten von Handys wiederherzustellen. Aber Toshiba hat vor einigen Wochen bereits Mini-Festplatten für Handys vorgestellt, die Ende des

Jahres in die ersten Telefone eingebaut werden sollen. So können nicht nur wenige Megabyte, sondern mehrere Gigabyte Daten im Handy untergebracht werden. Und auch hier wird wieder die Problematik des sicheren Löschsens der Daten eine Rolle spielen.

Gefahr des Datenmissbrauchs

Die Gefahr des Missbrauchs der Daten liegt nahe. So können Kontozugangsinformationen missbraucht werden, um Überweisungen vorzunehmen. Verwendet man die korrekten PIN und TAN, so hat der Kontoinhaber den Schaden zu tragen, denn er kann nicht oder nur schwer beweisen, dass nicht er den Auftrag zur Überweisung gegeben hat.

Die gefundenen Personaldokumente (Personalausweis, Führerschein, Geburtsurkunde) können Kriminellen ermöglichen, eine fremde Identität anzunehmen. Und letztlich können strafrechtlich relevante Daten (Raubkopien) sogar zu Erpressungen des ehemaligen Besitzers führen, z.B. der Familienvater, der seine Porno-Sammlung einschließlich Bildern mit Tieren, nur ungern an seine Ehefrau gesendet sehen möchte.

Bei dem Missbrauch der Daten der genannten Krankenkasse aber auch aller anderen Unternehmen können den Verantwortlichen sogar möglicherweise sowohl zivil- als auch strafrechtliche Konsequenzen aufgrund der Verletzung datenschutzrechtlicher Vorschriften und daraus resultierendem Schaden erwachsen.

Gegenmaßnahmen

Jedem PC-Benutzer muss klar sein, dass Löschen und Formatieren aus Windows die Daten nicht vernichtet. In dieser Studie wurden bereits Verfahren vorgestellt, die eine Wiederherstellung der Daten verhindern. Die minimale Anforderung zum Schutz der Daten ist deren Verschlüsselung, so dass die Daten nicht brauchbar sind. Wer auf Nummer Sicher gehen möchte, sollte die Daten mit einschlägiger Software sicher löschen. Es gibt zahlreiche

Anbieter im Internet, die solche Programme für wenig Geld anbieten.

Wer diesen Aufwand nicht betreiben möchte, sollte sich überlegen, ob er das nächste Mal die Festplatte nicht lieber vernichtet anstatt sie zu verkaufen. Aber auch hier ist Vorsicht geboten. Denn das bloße Wegwerfen in die Mülltonne bedeutet noch lange nicht, dass die Daten nie wieder auftauchen werden.

Danksagungen

An dieser Stelle möchte ich mich bei meinen Kollegen Frank Labedzki, André Weiß, Matthias Günther und Fatihelyasin Erdas für die Unterstützung bei der Durchführung der Studie bedanken. Sie haben nicht nur den wochenlangen Erwerb der Datenträger übernommen, sondern auch die zeitaufwendigen Datenrekonstruktionen und Ermittlung der Statistiken. Dank gilt auch meinem Kollegen Frank Alperstädt für die konstruktive Kritik an den Entwürfen dieser Studie.

Über den Autor

Diplom-Informatiker Olaf Kehrer ist Geschäftsführer der Berliner O&O Software GmbH, die sich unter anderem mit dem Thema sichere Datenlöschung beschäftigt. Er ist u.a. verantwortlich für die Entwicklung neuer Technologien und Produkte auf dem Gebiet der Datensicherheit. Hierzu zählen die Produkte O&O BlueCon, O&O SafeErase sowie O&O UnErase, die neben den in der Studie beschriebenen Lösungsverfahren auch die Wiederherstellung und Reparatur von Windows-Systemen ermöglichen.

Über die O&O Software GmbH

Die O&O Software GmbH entwickelt seit 1997 Tools für Windows, die mittlerweile in mehr als 80 Ländern in verschiedenen Sprachen eingesetzt werden. Zu ihren Kunden zählen Privatpersonen, klein- und mittelständige Unternehmen, aber auch öffentliche Einrichtungen und weltweit operierende Konzerne. Das Produktportfolio umfasst Applikationen zur Performanceoptimierung, 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

Internet: <http://www.oo-software.com/>

E-mail: info@oo-software.com

Telefon: +49 (0)30 4303 43-00

Fax: +49 (0)30 4303 43-99

Anhang A: Speichern und Löschen von Daten auf Festplatten

Der nachfolgende Text wurde bereits auszugsweise im April 2003 in einem Artikel des Autors bei tecchannel.de veröffentlicht.[8]

Wie werden Daten gespeichert

Bevor man Daten richtig 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 sog. Versionierungssysteme zu genießen, bei denen explizit alte Versionen von Dateien aufgehoben werden, um sie später z.B. 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 auch hier das Löschen dieser (Schatten-)Dateien notwendig, um die Daten vollständig zu vernichten.

Aber auch Windows selbst erstellt Kopien der Daten: temporäre Dateien beinhalten 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 norma-

lerweise keinen Zugriff hat. Eines dieser Probleme stellen die sog. Cluster Tips dar. Jede Festplatte wird beim Formatieren in Zuordnungseinheiten (Blöcke) unterteilt. Sie sind die kleinste Einheit einer Festplatte, der von dem Betriebssystem verwendet werden kann. 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 frei gegeben 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. Diese sei für unser Beispiel nur 10 KByte groß. Somit 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 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 Löschrprogramme können diese Bereiche gelöscht werden. Diese Verfahren werden 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 Rändern 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 ist ein erheblicher technischer und finanzieller Aufwand und sehr detailliertes Wissen notwendig, so dass vermutlich nur sehr gut ausgestattete Datenrettungsunternehmen oder auch 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 Daten – wenn auch mit mehr Aufwand – immer noch rekonstruiert werden können.

Ein- oder zweimaliges Überschreiben kann durch ein 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 oder 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 einer Differenz zum zugehörigen Digitalsignal Rückschlüsse auf die vorherigen Datenwerte ziehen. Denn wird eine 0 durch eine 0 überschrieben, so 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 Lösungsverfahren auch immer eine Kombination aus einem Datenwert und dessen Komplement, um das geschilderte Differenzverfahren unbrauchbar zu machen.

Anhang B: Literaturnachweis

- [1] 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>
- [2] 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
- [3] JOHN MARKOFF, “*Patient Files Turn Up in Used Computer*”, New York Times, 04.04.1997
- [4] MICROSOFT, “*Encrypting File System for Windows 2000*”, Microsoft Inc., Juli 1999; <http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp>
- [5] EGIL JULIUSSEN, PH.D., „COMPUTERS-IN-USE FORECAST“, eTForecasts, Juni 2000, http://www.etforecasts.com/products/ES_cinuse.htm
- [6] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, “*IT-Grundschutzhandbuch*”, BSI, 2003; <http://www.bsi.de/gshb/deutsch/menu.htm>
- [7] SIMSON L. GARFINKEL, ABHI SHELAT, “*Remembrance of Data Passed: A Study of Disk Sanitization Practices*”, Massachusetts Institute of Technology, 2003; <http://computer.org/security/>
- [8] MIKE HARTMANN, OLAF KEHRER, “*Daten sicher löschen*”, tecchannel.de, April 2003; <http://www.tecchannel.de/software/1161/index.html>