Studie zum Datenschutz bei gebrauchten Festplatten

Deutschland Deine Daten 2005

Dipl.-Inform. Olaf Kehrer, O&O Software GmbH, Berlin – Mai 2005

Wer heutzutage online geht, muss sich schützen. Immer mehr Betrüger tummeln sich im Netz und versuchen Bankzugangsdaten von gutgläubigen Nutzern zu erschleichen. Die IT-Industrie und die Bundesregierung haben darauf mit der Initiative "Deutschland sicher im Netz" reagiert[1]. Man kann dort wertvolle Tipps, wie man sich vor Betrügern, Spamern und Hackern schützt, nachlesen. Aber was passiert mit privaten und geschäftlichen Daten, wenn der Rechner nicht mehr gebraucht wird? Können diese Daten rekonstruiert und missbraucht werden? Diese Studie zeigt, was Sie beim Verkauf einer gebrauchten Festplatte unwissend aus der Hand geben können.

In unserer Studie im vergangenen Jahr haben wir 100 Festplatten bei eBay.de ersteigert und untersucht, ob sie noch Daten enthielten oder ob sie sicher gelöscht worden waren[2]. 88%[1] der funktionsfähigen Festplatten waren nicht richtig gelöscht, so dass nicht nur private und sehr persönliche Daten rekonstruiert werden konnten, sondern auch Patientendaten einer Krankenkasse, interne Dokumente eines Pharmakonzerns sowie Geschäftspapiere weiterer Unternehmen. Presse- und Fernsehberichte folgten und das Thema des sicheren Löschens von Daten auf gebrauchten Festplatten wurde vielen PC-Benutzern bewusst, die bisher davon ausgegangen waren, dass das Formatieren der Festplatte die Daten restlos vernichten würde. Eine fatale Fehlannahme, der aber auch durch die unklare Formulierung von Windows beim Formatieren der Festplatte Vorschub geleistet wird (siehe Abbildung 1).

Nicht nur der Angriff durch Viren, Trojaner und andere bösartige Programme stellen eine Bedrohung der Datensicherheit dar, sondern auch das ganz normale Entsorgen eines Rechners am Ende seiner Nutzungsdauer erfordert deshalb ein besonders geplantes und umsichtiges Vorgehen.

Ein Jahr nach der Veröffentlichung unserer ersten Studie wollten wir überprüfen, ob sich das Bewusstsein bei privaten PC-Benutzern als auch bei Firmen nachhaltig verbessert hat. Dafür haben wir erneut Festplatten ersteigert und mit Hilfe handelsüblicher Software auf nicht gelöschte Daten untersucht.

Ergebnisse aus 2004

Als wir im Jahre 2004 Festplatten ersteigerten, hätten wir niemals für möglich gehalten, welche brisanten Informationen darauf enthalten sein könnten. Eine der ersten Festplatten, die wir bekamen, enthielt Patientendaten einer Krankenkasse. Wie konnte es passieren, dass diese Festplatte zum Verkauf angeboten werden konnte?

Weitere Festplatten kamen hinzu mit sehr persönlichen und privaten Daten. Eingescannte EC-Karten, PINs, TANs, Kaufverträge, Arbeitszeugnisse und eine Entlassungsurkunde aus einer Justizvollzugsanstalt sind nur eine kleine Auswahl. Fotos und Filme von privaten Feiern und Urlauben gehörten genauso dazu wie private Pornosammlungen. Insgesamt über eine halbe Million Dateien konnten wieder hergestellt und ausgewertet werden.

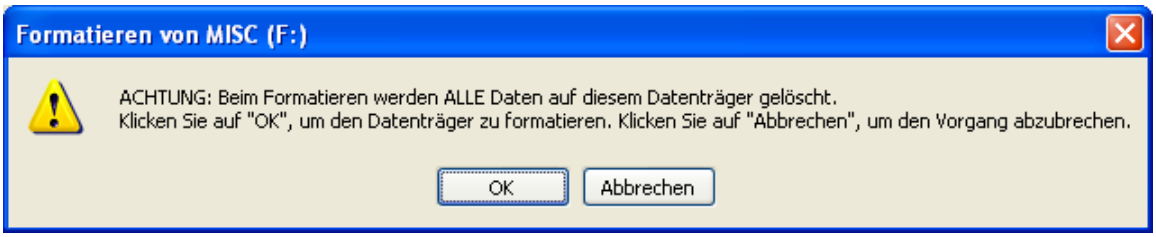
Und dies alles ohne besondere Hilfsmittel, nur mit gängiger Software, die jeder Windows-Anwender mit wenig Aufwand selbst benutzen kann.

Reaktionen

Auf die Veröffentlichung der Studie folgte ein breites Medienecho: Berichte im Magazin FOCUS, in der ARD („panorama“) und bei RTL („stern TV“) zeigten das Problem anhand von Bei-

[1] Es wurden 100 Festplatten untersucht, hiervon wiesen 15 einen physikalischen Defekt auf. Von den verbleibenden 85 Festplatten konnten auf 75 Daten wieder hergestellt werden. Dies entspricht einer Quote von ca. 88% der funktionsfähigen Festplatten oder auch 75% aller Festplatten.[2]

Abbildung 1: Der Warnhinweis vor dem Formatieren einer Festplatte ist irreführend



spielfällen und zeigten sehr deutlich, dass die Mehrzahl der Betroffenen sich diesen Vorgang nicht erklären konnte – „sie hätten doch die Festplatte vor dem Verkauf gelöscht“.

Dieses „Löschen“ war leider nur das Formatieren der Festplatte, das die Daten nicht wirklich löscht. Vergleicht man eine Festplatte mit einem Buch, dann entfernt Windows beim Formatieren nur das Inhaltsverzeichnis. Die Daten bleiben auf der Festplatte erhalten, lediglich der Verweis ist nicht mehr vorhanden. Als Benutzer kann man diese Daten dann auch nicht mehr sehen und auch nicht mehr darauf zugreifen. Dies gilt natürlich auch beim Löschen von Dateien. Diese werden normalerweise in den Papierkorb "geworfen", von wo aus man sie dann endgültig löschen kann. Auch hier gilt: es wird lediglich der Eintrag im Inhaltsverzeichnis entfernt, nicht jedoch die eigentlichen Daten.

Spezielle Datenrettungssoftware, wie O&O DiskRecovery oder O&O UnErase, kann diese Daten innerhalb kürzester Zeit wieder sicht- und somit lesbar machen.

Dies ist natürlich hilfreich, wenn man versehentlich Daten löscht, denn dann stehen die Daten schnell wieder zur Verfügung. Aber wenn man seine Festplatte verkauft oder verschenkt oder auch einfach nur in den Müll wirft, dann können Unbefugte diese Daten ebenfalls rekonstruieren und missbrauchen.

Wiederholung der Studie in 2005

Vor diesem Hintergrund haben wir uns die Frage gestellt, ob sich das Verhalten deutscher PC-Benutzer bzw. Verkäufer im Laufe des vergangenen Jahres verändert hat. Werden nun die Festplatten sicher gelöscht oder schlummern auf ihnen immer noch private und geschäftliche Geheimnisse?

Ergebnisse in 2005

Um dieser Frage nachzugehen, haben wir in den ersten Monaten dieses Jahres 200 Festplatten erneut bei eBay.de erworben und ausgewertet.

Insgesamt wurden 200 Festplatten mit einer Gesamtkapazität von 3,18 Terabyte (3.255 GByte) erworben. Damit wurde das Volumen der Festplatten von durchschnittlich 5,26 GByte auf 16,27 GByte mehr als verdreifacht.[2]

Von diesen 200 Festplatten waren 42 technisch defekt, was einer Quote von 21% und einer Steigerung von 6% gegenüber 2004 entspricht. Auch bei der diesjährigen Studie wurden defekte Festplatten nicht weiter betrachtet, da zu ihrer Rekonstruktion ein erhöhter Aufwand notwendig wäre. Diese Möglichkeit würde einem normalen PC-Nutzer nur eingeschränkt zur Verfügung stehen und ist daher für diese Studie nicht relevant.

Von den verbleibenden 158 Festplatten waren 45 sicher gelöscht, so dass keine Daten rekonstruiert werden konnten. Dies entspricht 28,5% und ist mehr als eine Verdopplung gegenüber 2004, als dieser Wert noch bei 11,7% lag. Ist dies bereits die Entwarnung? Nein, denn der überwältigende Rest von 113 Festplatten waren entweder gar nicht gelöscht oder nur formatiert worden.

Dies bedeutet, dass 71,5% der Festplatten persönliche und geschäftliche Daten enthielten, die rekonstruiert werden konnten.

Insgesamt wurden über 3,3 Millionen Dateien mit einer Gesamtgröße von 746 GByte von den

[2] In der Studie 2004 wurden 100 Festplatten mit einer Kapazität von 526 GByte erworben.

Festplatten wieder hergestellt. Darunter waren alleine 40.000 Word-Dokumente und knapp 15.000 Excel-Tabellen sowie ca. 50 Email-Postfächer mit dem gesamten Mailverkehr der vormaligen Nutzer.

Eines der „Highlights“ der diesjährigen Studie war eine Festplatte einer bundesdeutschen Behörde, die neben internen Berichten und Protokollen auch Schriftverkehr mit einer Ermittlungsbehörde enthielt. Daneben war auch die Festplatte einer deutschen Großbank enthalten, die unter anderem zahlreiche Dokumente mit der Bewertung der Kreditwürdigkeit (Rating) anderer Banken enthielt.

Nehmen wir Platz auf dem Sofa deutscher PC-Benutzer

Die Ergebnisse in 2004 waren alarmierend und wurden in 2005 nur geringfügig verbessert. Auch wenn objektiv die Quote der wieder herstellbaren Festplatten leicht gesunken ist, so ist die Qualität der Daten nach wie vor sehr hoch.

So kann man quasi mit einer alten Festplatte teilnehmen am Leben des vorherigen Besitzers, denn immer mehr alltägliche Dinge werden über den PC und das Internet abgewickelt. Von normalen Briefen über Ehescheidungen; von normalen Verabredungen per Email bis hin zu „erotischen“ Phantasien; von Arbeits- und Schulzeugnissen bis hin zu Kündigungen.

Und Dank des Zeitalters der digitalen Fotographie kann man sich auch noch ein Bild des arglosen Vorbesitzers machen. Im Kreise der Familie, bei der Weihnachtsfeier, im Urlaub oder auch mal ganz privat im Schlafzimmer. Und wenn das noch nicht reicht, so werden gleich komplette Pornosammlungen jeglicher Couleur mitgeliefert.

Machen wir es uns also bequem auf dem Sofa deutscher PC-Benutzer und tauchen wir ein in das Privatleben. Wofür ein guter Privatermittler Tage, vielleicht sogar Wochen gebraucht hätte, bekommen wir für knapp 30 Euro ins Haus geliefert. Und in nur ein paar Stunden sind sämtliche Geschichten, Anekdoten, Emails und Fotos rekonstruiert. Einfach, automatisch, schnell.

Zu Gast in deutschen Amtsstuben und Firmen

Aber nicht nur private Benutzer sind unvorsichtig mit ihren Daten. Das gleiche gilt auch für öffentliche Einrichtungen, Behörden, Firmen und sogar Banken.

Bundesdeutsche Behörde

So konnten wir in einem Fall Daten von einer Festplatte wieder herstellen, die offensichtlich zuvor in einer Niederlassung der Behörde eingesetzt worden war. Neben internen Papieren konnten auch personenbezogene Daten ermittelt werden. Insbe-

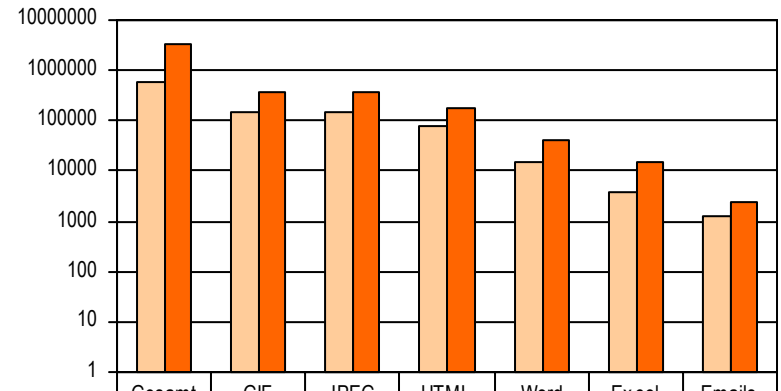
Abbildung 2: Gefundene Dateitypen

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

Knapp 40.000 Word- und fast 15.000 Excel -Dokumente waren lesbar (2004: ca. 15.000 und ca. 4.000).

Hinzu kamen über 50 Outlook-Postfächer (PST-Dateien) mit insgesamt über 2.000 Emails.

y-Achse der Tabelle ist logarithmisch aufgetragen



	Gesamt	GIF	JPEG	HTML	Word	Excel	Emails
Anzahl 2004	590000	149036	141633	78475	15248	3918	1271
Anzahl 2005	3334676	357691	359150	178156	39999	14639	2310

sondere die Korrespondenz zwischen dem Ermittlungsbeamten und der Behörde sowie mit einem Rechtsanwalt, der für einen Mandanten die Vertretungsvollmacht anzeigte, hätte in falschen Händen erheblichen Schaden anrichten können.

Reiseveranstalter

Eine weitere Festplatte stammte von einem bekannten Reiseveranstalter. Dort waren unter anderem Daten über die Abrechnung mit Buchungssystemen sowie die Konditionen, die Reisebüros bei Buchungen erhalten, zu lesen.

Nebenbei war auch noch die Kündigung der Zusammenarbeit mit einer Firma wegen schlechter Leistungen nachzulesen sowie der Neuabschluss des Vertrages mit deren Nachfolgern.

Kreditwürdigkeit anderer Banken gefällig?

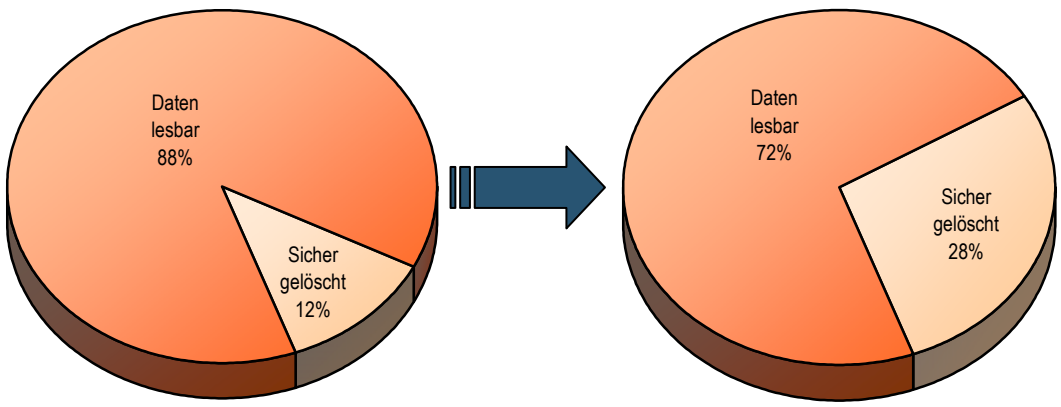
Ein weiteres „Bonbon“ war aus dem sensiblen Bereich der Finanzwelt. Zahllose interne Dokumente einer großen deutschen Bank tauchten bei unserer Recherche auf. Eine Vielzahl von Bewertungen anderer Banken und Institutionen in Bezug auf Kreditwürdigkeit und dem potenziellen Engagement der Bank waren dort nachzulesen. Für Mitbewerber sicher eine spannende Lektüre, wenn sie wissen, welche Strategien und Aspekte bei diesen Engagements im Vordergrund stehen.

„Zwiebelfestplatte“

Besonders interessant war auch eine Festplatte, die offensichtlich drei unterschiedliche Vorbesitzer hatte, die auch anscheinend nichts miteinander zu tun hatten. Diese „Zwiebelfestplatte“ enthielt Dokumente von einem Privatdetektiv, der mit der zuständigen Behörde über seine Zulassung Briefe ausgetauscht hatte. Des weiteren waren Angebotsdokumente von einem Büromaschinenvertrieb enthalten mit Kundendaten und Kalkulationen.

Die interessantesten Dokumente stammten jedoch von einem (ehemaligen) Geschäftsführer eines mittelständischen Unternehmens, in denen das Zerwürfnis mit anderen Geschäftsführern und Gesellschaftern in Protokollen akribisch festgehalten wurde. Von normalem Briefwechseln über Anschuldigungen bis hin zum Vorwurf der Untreue und des vorsätzlichen Kapitalentzugs durch beteiligte Gesellschafter konnte man das Schicksal des Unternehmens bis zur möglichen Insolvenz verfolgen. Ferner waren noch interne Stundungsvereinbarungen über beträchtliche Beträge und eine Liste potenzieller Kapitalgeber und deren Akquisitionsstatus enthalten. Insgesamt äußerst brisantes Material, das sicherlich niemals hätte veräußert werden dürfen.

Abbildung 3: Wiederherstellungsquote von funktionsfähigen Festplatten



In 2004 waren 88% der funktionsfähigen Festplatten lesbar (75% aller Festplatten), wobei die Quote der defekten Festplatten mit nur 10% deutlich geringer war als in 2005. In 2005 waren immer noch 72% der Festplatten lesbar.

Welche Ursachen führen zu dieser Unvorsichtigkeit?

Unwissenheit ist das Hauptproblem

Nach wie vor gehen wir davon aus, dass die meisten Benutzer fest davon überzeugt sind, dass sie ihre Daten gelöscht hatten. Windows suggeriert dies ja auch durch seine Meldung beim Formatieren, dass alle Daten unwiderruflich gelöscht werden. Hier besteht also hoher Aufklärungsbedarf, dass zusätzliche Maßnahmen dringend notwendig sind, um die Daten wirklich sicher zu löschen.

Erstaunlich ist auch, dass wir häufig von Administratoren in Firmen hören, dass alle Daten zentral auf einem Server gespeichert werden und lokal keine wichtigen Daten liegen. Deshalb sind spezielle Löschmaßnahmen bei Festplatten von Arbeitsplatzrechnern nicht erforderlich. Eine gefährliche Annahme, denn hier lauern gleich mehrere Gefahren.

Zum einen muss sichergestellt werden, dass Daten nicht wirklich lokal gespeichert werden. Dies ist mit erheblichem Aufwand verbunden und wird deshalb in der Regel gar nicht oder nur unvollständig durchgeführt. Hinzu kommt der lokale Zwischenspeicher von Daten (sog. Cache), der beispielsweise beim Surfen im Internet verwendet wird. Werden Daten von Intranet-Servern abgerufen, dann werden sie auch lokal zwischengespeichert. Diese Daten können hochsensibel sein und müssen somit ebenfalls sicher gelöscht werden.

Hinzu kommen noch temporäre Dateien beispielsweise von Textverarbeitungs-, Tabellenkalkulations- und Datenbankprogrammen, die normalerweise auch lokal abgelegt werden. Auch hier können sensible Daten später rekonstruiert werden.

Unachtsamer Umgang mit Festplatten

Ein weiteres Problem ist der Umgang mit Festplatten und allen anderen Datenträgern. Im Falle eines Defekts wird meist der gesamte Rechner zum Händler retourniert – inklusive der zugehörigen Festplatte.

Vielen ist gar nicht bewusst, dass sie private und sensible Daten in fremde Hände geben. Insbesondere dann, wenn aufgrund des Defekts der gesamte Rechner oder auch „nur“ die Festplatte ausgetauscht werden. Wo bleibt die alte Festplatte mit den Daten? Es kann durchaus zu einem „Recycling“ dieser Festplatte kommen, wie ein aktueller Fall im RTL-Magazin „EXTRA“ vom 7. März 2005 gezeigt hat. Hier hatte ein Käufer eines PC-Systems auf der angeblich neuen Festplatte Daten seines Vorbesitzers gefunden und diesen anhand von persönlichen Schreiben ermitteln können. Vielleicht ein Einzelfall, aber bei allen Reparaturen am PC-System ist immer sicherzustellen, dass wichtige Daten nicht unkontrolliert in fremde Hände gelangen!

Gegenmaßnahmen

Bereits in der vorherigen Studie hatten wir verschiedene Methoden zur Vermeidung der Wiederherstellung der Daten beschrieben[2]. Von der Verschlüsselung der Festplatte über die physikalische Zerstörung des Datenträgers bis hin zum Einsatz spezieller Löschsoftware existieren eine Reihe von Verfahren, die alle Vor- und Nachteile besitzen.

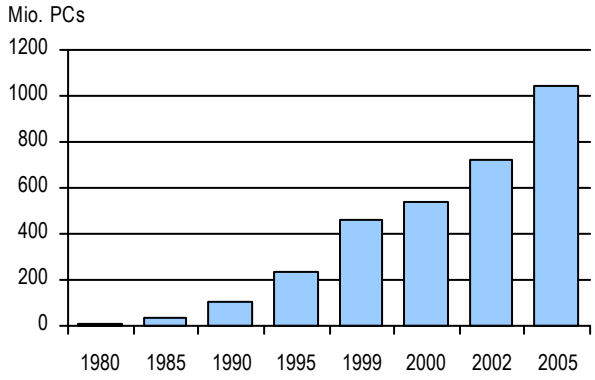
Aufgrund der Reaktionen der Leser der Studie des vergangenen Jahres können wir sagen, dass das sichere Löschen mittels spezieller Software mit Abstand die gebräuchlichste Methode ist, so dass wir die anderen Verfahren hier nicht weiter betrachten wollen. Den interessierten Leser verweisen wir gerne auf die Studie, die auch detaillierte Informationen zum Speicherprozess von Festplatten enthält.[2]

Formatieren reicht nicht!

Nach wie vor erliegen viele PC-Nutzer dem Trugschluss, dass das Formatieren die Festplatte endgültig löschen würde. Dies ist falsch, denn Windows löscht nur das Inhaltsverzeichnis, nicht jedoch den Inhalt der Festplatte, wie bereits beschrieben wurde.

Um wirklich sicher gehen zu können, dass die Daten vernichtet werden, muss eine zusätzliche Software eingesetzt werden. Diese sollte mindestens nach einem der international anerkannten Standards Daten löschen können. Dabei wird eine bestimmte Anzahl von Löschvorgängen, was dem Überschreiben der ursprünglichen Daten mit vordefinierten Mustern entspricht, definiert. Diese müssen in einer bestimmten Reihenfolge durchgeführt werden, um auch die Wiederherstellung mittels Hardware zu erschweren bzw. unmöglich zu machen. Der Einsatz einer solchen Software ist sehr einfach und effizient durchzuführen.

Abbildung 4: Anzahl installierter PC-Systeme weltweit [5]



Standardisierte Verfahren zum Löschen

Diese Verfahren sind zum einen vom US-amerikanischen Verteidigungsministerium (Department of Defense, DoD), zum anderen vom neuseeländischen Experten Peter Gutmann, der ein bis zu 35maliges Überschreiben für die endgültige Vernichtung aller Daten favorisiert, beschrieben worden.[3][4]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ebenfalls einen entsprechenden Standard definiert.[5] Achten Sie deshalb unbedingt darauf, dass die von Ihnen verwendete Löschsoftware diese Verfahren unterstützt.[3]

Fazit

Jeder Mensch hängt an Erinnerungen, das ist vollkommen normal. Man möchte so viele von ihnen wie möglich behalten und für die Ewigkeit archivieren. Früher hat man dies mit Briefen oder Postkarten, mit Fotos oder einfach nur Erzählungen von Geschichten und Ereignissen getan. Heute schreibt man Emails oder SMS, erstellt digitale Fotos oder Videoaufnahmen und schreibt seine Gedanken in Textdokumenten oder Internet-Foren nieder.

Das hat natürlich eine Vielzahl von Vorteilen und keiner möchte heute mehr ohne diese Errungenschaften der Informationstechnik leben. Dies ist an sich auch nicht problematisch, aber man muss sich der Risiken bewusst sein. Täglich kann man in Magazinen, Tageszeitungen und Online-Nachrichten von Virenangriffen, Phising-Attacken[4] und Trojanern lesen, die Kennwörter ausspähen wollen. Dagegen kann man sich zwar mit spezieller Software zum Großteil schützen, aber dennoch ist ein umsichtiger Umgang mit wertvollen Informationen wie Online- und Bankzugängen zwingende Voraussetzung für die Minimierung der Risiken. Und dazu zählt letztendlich auch die Entsorgung von Datenträgern am Ende ihres Lebenszyklus. Nicht nur Festplatten, sondern auch Disketten, USB-Sticks, Memory-Cards und alle weiteren Datenspeicher sollten nicht achtlos weggeworfen, verschenkt oder verkauft werden. Stellen Sie immer sicher, dass alle Daten sicher gelöscht sind. Und gehen Sie nicht einfach davon aus, dass die Daten nicht wichtig oder für andere nicht interessant sind.

Zusammenfassung und Vergleich mit 2004

Im Jahr 2004 wurden laut Gartner weltweit 189 Millionen PCs verkauft. Das sind 11,8 Prozent mehr als 2003 und auch in 2005 zeichnet sich eine erneute Steigerung ab.[7]

Neue PC-Systeme bedeuten heutzutage nicht mehr primär, dass es sich hierbei um Erstanwender handelt, sondern dass alte PC-Systeme ersetzt werden. Es werden immer schneller neue und leistungsfähigere Speichertechniken entwickelt und in den Markt gebracht als dies noch vor Jahren der Fall war.

Handys speichern Emails, Kontakte, Fotos und vieles mehr. USB-Sticks sind Mini-Datenspeicher mit gigantischem Fassungsvermögen, die problemlos eine ganze Enzyklopädie speichern können. Und die momentan überaus „trendigen“ MP3-Player können auch viel mehr als nur Musik speichern und abspielen. Überall im täglichen Leben findet man Datenspeicher, die häufig persönliche Daten enthalten, ohne dass es einem wirklich bewusst ist.

Der stetige Preisverfall im IT-Bereich macht es uns auch leicht, ein neues PC-System zu erwerben. Die Daten vom alten PC werden noch schnell auf das neue System kopiert und dann geht es entweder zu

[3] O&O SafeErase V2.0 unterstützt alle vorgestellten Verfahren sowie zusätzlich weitere Verfahren zum sicheren Löschen von Dateien, Festplatten und kompletten Rechnern.

[4] Beim **Phising** versucht ein Betrüger, Internet-Benutzer durch gefälschte Emails oder andere Tricks dazu zu bringen, gefälschte Websites zu besuchen und dort persönliche Informationen wie Bankzugangsdaten, Kreditkartennummern oder ähnliches einzugeben.[8]

Freunden und Bekannten oder via Internet zu einem neuen (fremden) Besitzer.

Wo das System letztendlich „landet“, ist ungewiss. Und genauso ungewiss ist, ob unvollständig gelöschte Daten nicht doch missbraucht werden könnten. Wie würden Sie es finden, wenn andere Leute in Ihrer Mülltonne wühlen und nach Briefen, Kontoauszügen, Rechnungen oder gar Mahnungen suchen würden?

Gefahr des Missbrauchs

Wenn jemand Ihre persönlichen Zugangsdaten missbraucht, dann kann er damit sogar die Identität der ahnungslosen Person annehmen. Er kann für sie im Internet einkaufen, Dinge ersteigern oder einfach nur Emails schreiben. Das kann verheerende Konsequenzen haben, zumal der Geschädigte nachweisen muss, dass die Bestellungen und Emails nicht von ihm stammen. Das kostet Zeit, Geld und kann zusätzlich eine Menge Unannehmlichkeiten bedeuten.

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

Hier 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 des Unternehmens darstellen.

Was bei privaten Daten vielleicht einfach nur ärgerlich ist, kann bei geschäftlichen Daten den Ruin bedeuten. Eine Veröffentlichung interner Daten kann schnell zu zivil- und sogar strafrechtlichen Konsequenzen führen. Personenbezogene Daten mit Einzelheiten über Auftraggeber und Auftragnehmer haben wir auch dieses Jahr wieder gefunden. Würden diese Daten in 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 Mitbewerber.

Jeden Tag ein Geheimnis

Allein bei dem deutschen Ableger der Auktionsplattform eBay gibt es täglich über 5.000 Festplatten zu ersteigern. Angesichts unserer Studienergebnisse ist weiterhin davon auszugehen, dass bei einer Vielzahl davon ungewollt private und geschäftliche Informationen weiter gegeben werden.

Löschen! Löschen! Löschen!

Es gibt nur eine Möglichkeit, den Datenmissbrauch zu vermeiden: Löschen Sie alle Datenträger immer mit spezieller Software, bevor Sie sie weiter geben. Oder vernichten Sie die Datenträger durch physikalische Zerstörung. Für welche Möglichkeit Sie sich auch entscheiden, bedenken Sie immer, dass das einfache Löschen mit Windows niemals ausreichend ist! *[OK]*

Impressum

Danksagungen

An dieser Stelle möchte ich mich bei meinen Kollegen Frank Witter, 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 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 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.

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 internationale 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

Literaturnachweis

[1] MICROSOFT DEUTSCHLAND GMBH, *"Deutschland sicher im Netz"; http://www.sicher-im-netz.de*

[2] OLAF KEHRER, O&O SOFTWARE GMBH, *"Deutschland Deine Daten",* April 2004; http://www.oo-software.com/de/study/

[3] 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

[4] 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

[5] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, *" IT-Grundschutzhandbuch"*, BSI, 2003; http://www.bsi.de/gshb/deutsch/menue.htm

[6] EGIL JULIUSSEN, PH.D., „COMPUTERS-IN-USE FORECAST", eTForecasts, Juni 2000, http://www.etforecasts.com/products/ES_cinuse.htm

[7] NETZZEITUNG, *"PC-Absatz wuchs 2004 zweistellig"*, 19. Januar 2005; http://www.netzeitung.de/spezial/globalvillage/321693.html

[8] WIKIPEDIA, *"Phising"*; http://de.wikipedia.org/wiki/Phishing