Wirklich alles gelöscht?

Heikle Daten auf gebrauchten Platten, Smartphones und Druckern

Schon für zehn bis zwanzig Euro bekommt man gebrauchte Festplatten auf eBay, Smartphones bringen je nach Alter nur unwesentlich mehr Geld. Offenbar zu wenig, als dass es den Verkäufern wert wäre, Zeit zum sorgfältigen Löschen ihrer Daten zu investieren: Unsere Funde übertrafen die ärgsten Befürchtungen.

Von Mirko Dölle und Alexander Spier

Für die zu klein gewordene Festplatte, das bei der letzten Vertragsverlängerung übrig gebliebene Smartphone oder den alten Firmenkopierer bekommt man auf eBay kaum mehr als ein Taschengeld. Doch viele Elektronikgeräte, insbesondere Datenträger, enthalten äußerst private Informationen, die man als Verkäufer löschen muss, damit sie nicht in falsche Hände geraten.

Doch wie sieht die Praxis aus? Löschen Verkäufer die Datenträger wirklich vollständig? Wir haben inkognito bei eBay ein halbes Dutzend gebrauchte Festplatten, drei ältere Android-Smartphones und einen Firmenkopierer von Privatpersonen aus Deutschland und aus Österreich gekauft. Mit Photorec und foremost haben wir zwei Open-Source-Forensikprogramme in Stellung gebracht, die mühelos die Daten von leichtfertig formatierten Festplatten rekonstruieren. Damit untersuchten wir die Geräte auf Datenreste der Vorbesitzer. Das Ergebnis übertraf unsere ärgsten Befürchtungen um Längen.

So hätten wir uns bei der Hälfte der Festplatten die Installation der Forensikprogramme sparen können: Die Vorbesitzer machten sich nicht einmal die Mühe, ihre privaten Dateien und Dokumente in den Papierkorb zu befördern, geschweige denn, die Festplatten zu formatieren. Sie bauten die Laufwerke einfach aus und schickten sie uns. Die anderen waren lediglich schnellformatiert worden, sodass Photorec Hunderttausende Dateien und Verzeichnisse, mitunter sogar mit dem Original-Dateinamen, wiederherstellen konnte. Vollständig überschrieben war nicht eine einzige Festplatte, auch nicht die aus dem Firmendrucker. Somit gelangten wir in den Besitz ansehnlicher Datenbestände.

Eine Gamer-Festplatte machte den Anfang. Die Vorbesitzerin aus der Gegend von Berlin hatte sie mit NTFS schnellformatiert. Offenbar spielt sie vorwiegend Call of Duty und Battlefield 3, was etliche Screenshots und Videos ihrer Partien nahelegen. Wir hätten damit ihre Mitspieler und Gegner identifizieren können, davon abgesehen fanden wir aber keine privaten Dokumente, Fotos oder Videos.

Doppelfehler

Aus dem Süden Baden-Württembergs kauften wir ein defektes NAS mit gleich zwei 1-TByte-Festplatten. Mit einem Reparaturversuch hielten wir uns gar nicht erst auf, sondern demontierten kurzerhand die beiden Laufwerke. Ungewöhnlich war, dass es sich um zwei verschiedene Festplatten von zwei Herstellern und sehr unterschiedlichen Produktionsjahren handelte: die eine war 2009, die andere 2012 hergestellt worden. Offenkundig hatte der Verkäufer die bislang im NAS betriebenen Festplatten ausgebaut und gegen andere, ältere ersetzt. Für uns ein Glücksfall, denn so bekamen wir nicht zwei Festplatten eines RAID-1-Verbunds mit identischen Daten, sondern zwei als PC-Festplatten genutzte Laufwerke, die unterschiedliche und damit unterm Strich mehr private Daten enthielten als ein RAID-Verbund.

Auf der ersten Festplatte fanden wir ein völlig unbeschädigtes NTFS-Dateisystem mit diversen Spielen vor. Besonders

Schnäppchen allenthalben: Ein halbes Dutzend Festplatten für maximal 30 Euro inklusive Versand, drei Android-Smartphones für unter 150 Euro und einen ebenso günstigen Firmendrucker haben wir bei eBay ersteigert – und mit ihnen eine Menge Daten.

Intime Fotos wie hier von der Geburt der Kinder oder beim Planschen im Garten haben in Händen Dritter nichts verloren.

aktiv war der Vorbesitzer bei League of Legends, hiervon fanden wir etliche Videos, Screenshots sowie Chat-Protokolle. Noch aufschlussreicher war die zweite Festplatte. Sie war mit NTFS schnellformatiert worden, aber Photorec hatte keine Schwierigkeiten, Hunderttausende Dateien wiederherzustellen. Darunter befanden sich nicht nur eine ansehnliche Porno-Sammlung, PGP-Schlüssel und eine vollständige Firefox-Konfiguration nebst Passwörtern, sondern auch die Konstruktionsbeschreibung eines klappbaren Siebgitters für Förderkübel, die Lebensläufe von Sohn und Vater, ein Praktikumstagebuch, diverse private Skype-Chat-Logs, Kontaktdaten von WhatsApp- und Facebook-Freunden und ein wenig versöhnliches Testament der Mutter.

Schwäbische Sparsamkeit

Auch unsere Festplatte aus dem Schwabenland stammte aus einem NAS und wurde wohl in Folge eines Upgrades ausgemustert und bei eBay angeboten – genau wie ihr Zwilling, denn es handelte sich um einen RAID-1-Verbund. Der Verkäufer, pikanterweise ein IT-Consultant und ehemaliger c't-Abonnent, hatte unser Laufwerk lediglich von dem NAS neu formatieren lassen. Da es sich um ein NAS mit Linux-Firmware handelte und ein Ext3-Dateisystem zum Einsatz kam, gelang es Photorec nicht nur, die Dateien selbst wiederherzustellen, sondern auch die Dateinamen und ganze Verzeichnisse. Das erleichterte uns die anschließende Analyse sehr.

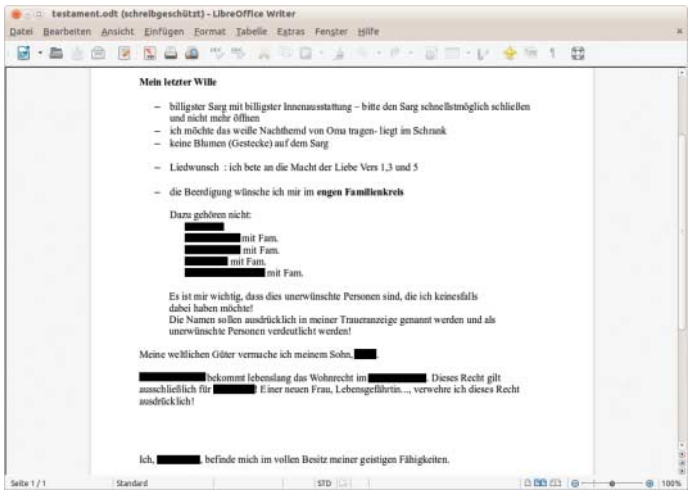
Unsere Ausbeute war enorm. Wir fanden ein über 200 GByte umfassendes Mail-Archiv, Personaldokumente nebst Diplomen und Zeugnissen vom Verkäufer und seiner Frau, Bewerbungen, Lebensläufe, Arbeitsverträge, eine strafbewehrte Unterlassungserklärung und einen Geheimhaltungsvertrag aus dem IT-Bereich. Die Bilder- und Videosammlung umfasste mehrere zehntausend Dateien und zeigte nicht nur intime Fotos seiner Frau und von der Geburt seines ersten Sohns, sondern auch der nackt planschenden Kinder im Garten. Zudem fanden wir interne Dokumente einer BOS-Hilfsorganisation, in der der Verkäufer offenbar eine Führungsposition bekleidet, sowie Hunderte nicht zur Veröffentlichung bestimmte Fotos von Einsätzen, deren unerlaubte Weitergabe als Verletzung der Verpflichtungserklärung nach dem Verpflichtungsgesetz angesehen und mit bis zu fünf Jahre Freiheitsstrafe geahndet werden könnte.

Für Kriminelle wären die detaillierten Bauzeichnungen des Wohnhauses des Verkäufers sowie Grundrisszeichnungen von Mietwohnungen von Interesse – eine exakte Ortskenntnis vorab erleichtert Einbrechern das Handwerk enorm. Zum Glück für den Verkäufer gehen die Autoren dieses Artikels einer anderen Beschäftigung nach. Dummerweise gibt es aber wie bereits erwähnt noch eine zweite, höchstwahrscheinlich mit unserer identische Festplatte, die in einer zweiten Auktion auf eBay verkauft – und definitiv nicht von uns erworben wurde. Es gibt also noch eine Person, die eine Kopie der von uns gefundenen Daten besitzt.

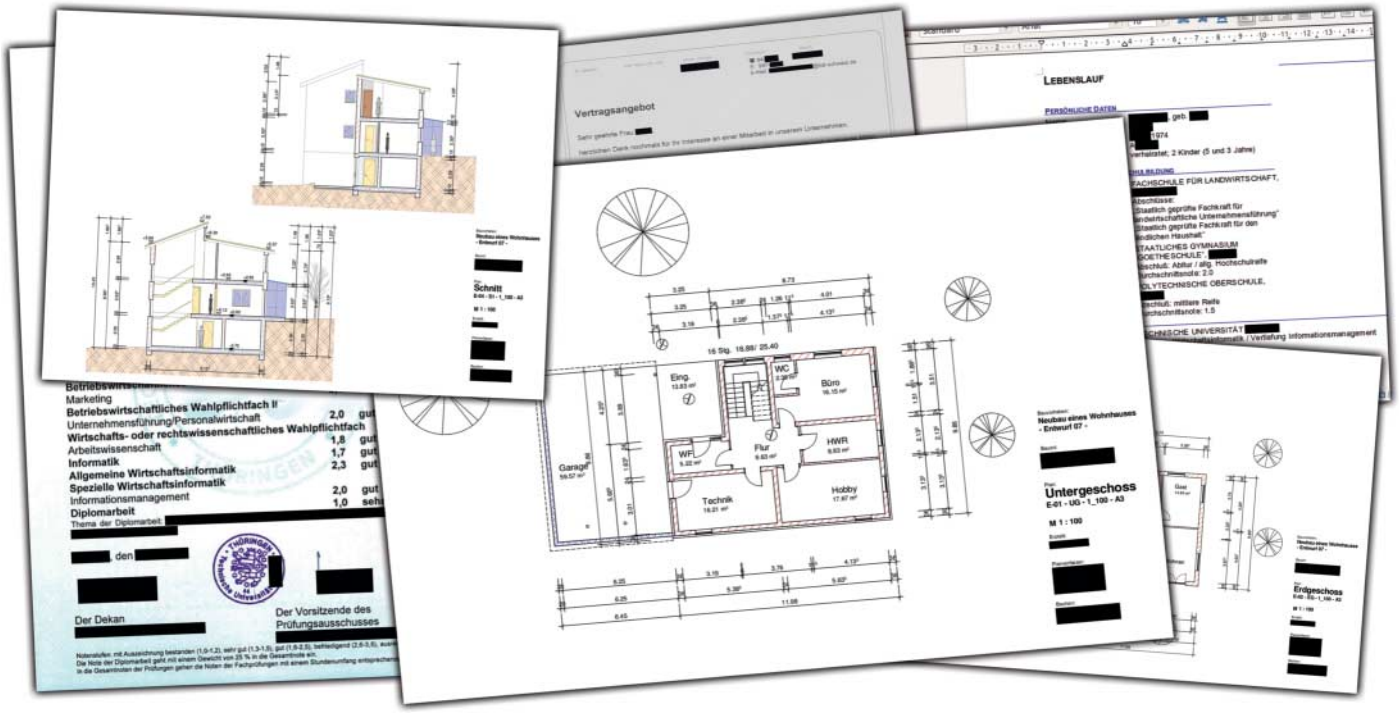
Bayerische Freizügigkeit

Was die Menge höchst intimer Daten angeht, schossen wir mit der Festplatte aus München den Vogel ab. Die Sorglosigkeit des Verkäufers machte uns sprachlos, denn obwohl sich höchst vertrauliche Daten wie Dutzende im Browser gespeicherte Passwörter und Kontoauszüge auf dem Laufwerk befanden, unternahm er nicht einmal den Versuch, irgend etwas zu löschen – wie erhielten ein bootfähiges, einwandfrei funktionierendes Windows-Laufwerk.

Doch das alles war harmlos im Vergleich zu dem, was im iTunes-Verzeichnis gespeichert war: Zwei vollständige und noch dazu unverschlüsselte Backups seines iPhones. Und auch dabei waren die iMessage-Datenbank, Telefon- und WhatsApp-Kontakte, Anrufhistorie und Browser-History die unbedeutendsten Funde. Wie sich herausstellte, fotografiert der Verkäufer gern und häufig seine Freundin, etwa leicht oder unbekleidet auf dem Bett. Sie posiert nicht nur, sie scheint außerdem ein regelrechter Selfie-Junkie zu sein, die sich gerne in knappen Dessous selbst fotografiert – etwa vor dem heimischen Wandspiegel oder in der



Dieses wenig versöhnliche Testament war wohl kaum für fremde Augen bestimmt. Photorec fand es mühelos auf der zweiten der im defekten NAS verbauten Festplatte.



Für Identitätsdiebe wären die Daten von Bildungsabschlüssen, Arbeitsverträgen und aus Lebensläufen einer der Festplatten sehr aufschlussreich; Einbrecher könnten sich dank detaillierter Baupläne des Wohnhauses bestens auf eine Tat vorbereiten.

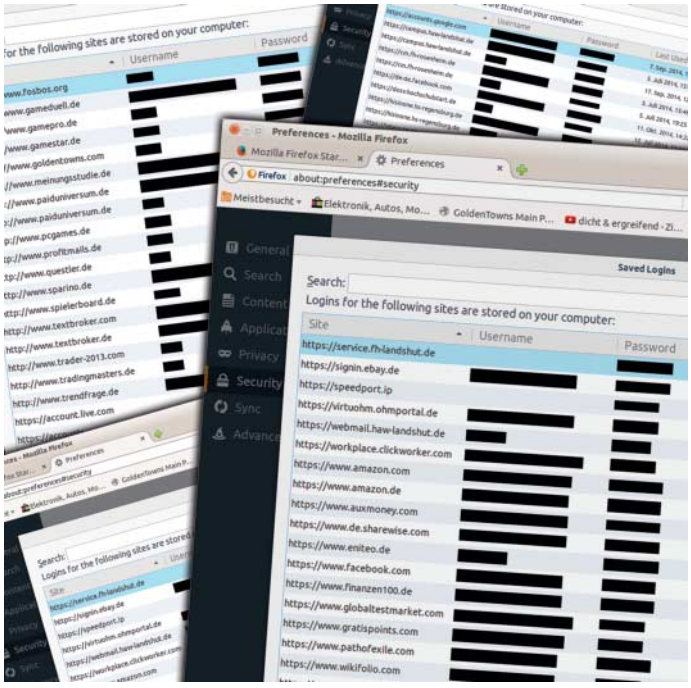
Umkleidekabine von Läden. Das Ergebnis war eine ganze Dessous-Modeschau mit fast fünfzig Bildern, ein Dutzend Bilder mit Reizwäsche und zwei Dutzend oben oder ganz ohne. Auch auf dem Bett und unter der Dusche entstanden einige Groß- und Detailaufnahmen, wir kennen sogar das Ergebnis des Schwangerschaftstests.

Das Bildmaterial würde sich nicht nur eignen, um es auf diversen Sex-Portalen hochzuladen, dank der Kontaktdaten und anderer Dokumente kennen wir auch die Identität der Freundin – ein Krimineller könnte die Festplatteninhalte auch für eine veritable Erpressung missbrauchen. Dass ihr Freund diese Fotos einem Fremden auf seiner alten Festplatte schickt, hat sich die Freundin wohl nicht gedacht.

Fünf zum Preis von einer

Der krasseste Fall war eine Notebook-Festplatte aus Österreich: Der Verkäufer betonte in der eBay-Auktion sogar explizit, dass die Festplatte nicht formatiert sei – die mussten wir einfach ersteigern. So erreichte uns eine bootfähigen Windows-Installation ohne Admin-Passwort, dafür mit etlichen im Browser gespeicherten Passwörtern und mit sämtlichen Dateien des Vorbesitzers. Der Rechner wurde offenbar hauptsächlich als Schreibmaschine im Schriftverkehr mit Behörden benutzt, besonders aufschlussreich war dementsprechend das Verzeichnis Documents des einzigen angelegten Benutzers.

Dort fanden wir Unterlagen zum Beantragen von Sozialleistungen nebst den üblichen Anlagen von insgesamt fünf Personen aus der Familie des Vorbesitzers – Kopien der Ausweise, Geburtsurkunden, Staatsbürgerschaftsnachweise, Meldebescheinigungen, Sozialversicherungskarten, Einkommensnachweise, Pensionsmitteilungen und sogar ein Sozialgerichtsurteil nebst Begründung. Die hohe Auflösung



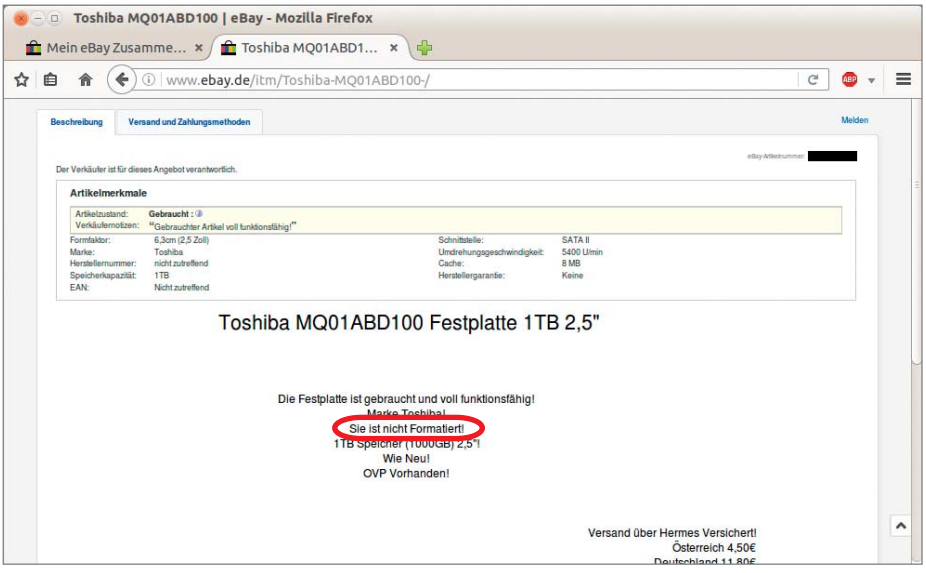
Auf der bootfähigen Windows-Festplatte waren Dutzende Zugangsdaten zu Websites sowie zum Mail-Account gespeichert, die uns Firefox bereitwillig im Klartext anzeigte.

Bilderbuch-Partnerschaft: Nicht nur der Vorbesitzer unserer Festplatte aus Bayern fotografiert gern seine Freundin, sie scheint ein Selfie-Junkie zu sein und schickt ihm häufig Bilder – vorzugsweise in knappen Dessous vor dem Spiegel, manchmal auch ohne und manchmal Detailaufnahmen aus der Dusche.

der Scans von 200 dpi könnte Kriminellen durchaus zur Herstellung von Fälschungen genügen, wenn sie sich nicht damit begnügen, sich falsche digitale Identitäten zu verschaffen oder sich die eBay- und Amazon-Konten unter den Nagel zu reißen und einfach auf Rechnung der Familie des Festplatten-Vorbesitzers einkaufen zu gehen – dank der gespeicherten Zugangsdaten hätte man vermutlich auch freien Zugriff auf sein E-Mail-Konto für Anmeldungsbestätigungen oder Benachrichtigungen. Ausprobiert haben wir das selbstverständlich nicht, das wäre illegal.

Kopie aus dem Kopierer

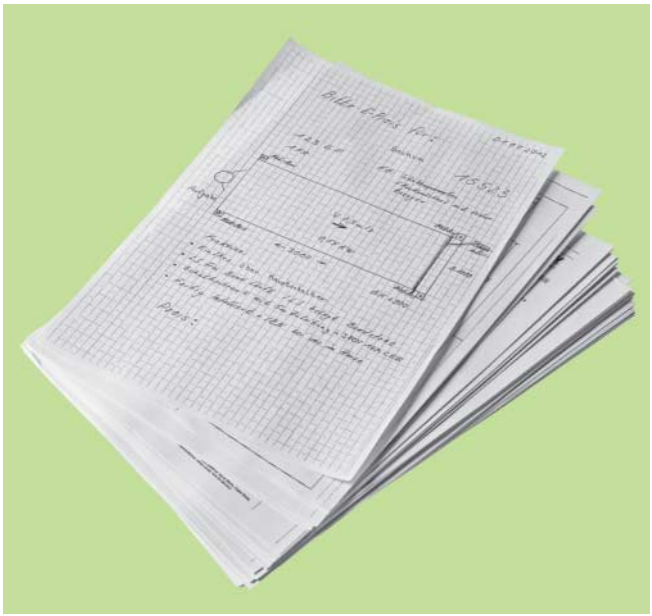
Festplatten finden sich nicht nur in PCs, sondern auch in digitalen Kopierern und Gruppen-Multifunktionsgeräten mit Scanner, Fax und Drucker. Deshalb ersteigerten wir ein ungefähr zehn Jahre altes Laser-Multifunktionsgerät für knapp 150 Euro. Und wieder mussten wir feststellen, dass es viel leichter war als gedacht: Niemand hatte sich die Mühe gemacht, die 40 GByte große Notebook-Festplatte anzutasten, nicht einmal die über das Bedienfeld leicht zugänglichen Fax- und Scan-Folder hatte man geleert. So konnten wir binnen Minuten feststellen, dass unser Gerät zuvor bei bei einem norddeutschen Fördertechnik- und Automationsbetrieb im Einsatz war – und fast 100 Seiten Faxe und Scans mit internen Unterlagen der Firma und von Kunden wie Volkswagen ausdrucken. Der einzige Wermutstropfen war, dass ein Admin Druckjobs nicht auf der Festplatte speichern ließ, sonst wäre die Ausbeute wesentlich höher gewesen. Zudem offenbarte uns das Web-Frontend ein umfangreiches Kommunikationsverzeichnis mit Hunderten Faxnummern empfangener oder gesendeter Faxe.



Kaum zu fassen: Der Verkäufer aus Österreich wirbt auf eBay sogar explizit damit, dass er das Laufwerk nicht formatieren wird. Wir fanden die kompletten Unterlagen von gleich fünf Personen auf dieser Festplatte.

Bilderbuch-Smartphone

Nicht nur Backups von Smartphones versprechen persönliche Daten, sondern auch die Smartphones selbst. Allerdings mit Einschränkungen: So verschlüsselt iOS den Flash-Speicher von Apple-Mobilgeräten bereits seit geraumer Zeit – setzt der Verkäufer das Gerät vor dem Versand auf die Werkseinstellungen zurück, hat man ohne den Schlüssel keinen Zugriff mehr auf die zuvor gespeicherten Inhalte. Genauso ist es bei Smartphones ab Android 6.



Fast 100 Seiten Faxe und Scans mit internen Unterlagen und Konstruktionszeichnungen sowie Kommunikation mit Kunden wie Volkswagen konnten wir mühelos dem gebrauchten Laser-Multifunktionsdrucker entlocken.

Deshalb entschieden wir uns zum Kauf von drei älteren Android-Smartphones.

Zwei kamen bereits mit installiertem Android 4.4 und waren von den Verkäufern auf die Werkseinstellungen zurückgesetzt worden. Obwohl der Flash-Speicher mutmaßlich nicht verschlüsselt war, kamen wir trotzdem nicht an die früheren Inhalte heran – Android nutzt seit Version 4.3 die Trim-Funktion des Flash-Controllers, sodass der Controller gelöschte Bereiche nach und nach von sich aus bereinigt.

Das von einem gewerblichen Anbieter ersteigerte Sony Xperia sola hingegen lief noch mit Android 2.3, sodass der Flash-Speicher durch das Zurücksetzen allein nicht vollständig gelöscht wurde. Der Zugriff darauf war allerdings nur per MTP möglich, sodass wir uns zunächst Root-Zugriff auf das Android-System verschaffen mussten, um ein Image des Flash-Speichers zu erstellen. Dazu nutzt man entweder eine der vielen bekannten Bootloader-Lücken älterer Android-Systeme aus oder entsperrt wie in unserem Fall mit einem vom Gerätehersteller bereitgestellten Code den Bootloader.

Mit der nachinstallierten Linux-Tool-Sammlung Busybox erstellten wir dann ein Abbild vom internen Speicher. Photorec fand darin über tausend Bilder und jede Menge Fragmente persönlicher Daten der Vorbesitzerin aus Nordrhein-Westfalen. Genug, um ihren Arbeitsplatz eindeutig zu identifizieren – ein abfotografiertes Amazon-Paket machte es möglich.

Passend zum Beruf der Vorbesitzerin entdeckten wir auch etliche Bilder von Häusern, Wohnungen sowie einige Grundrisse auf dem Gerät. Ein umfangreiches privates Adressbuch mit Namen, Telefonnummern und E-Mail-Adressen war ebenfalls unbeschädigt. Der Besuch auf dem Konzert der Toten Hosen hinterließ ein Video, ein WhatsApp-Chatlog gab Auskunft über vergangene Verabredungen, zudem gab es reichlich Katzen-Videos und -Bilder ihres Haustieres. Intime Details oder Geschäftsgeheimnisse tauchten in unserer Suche immerhin nicht auf.

Fazit

Unser Test zeigt: Den Begriff Formatieren setzen selbst IT-Fachleute häufig mit sicherer Datenlöschung gleich – und wiegen sich in trügerischer Sicherheit. Dabei bedeutet Formatieren tatsächlich nur die Vorbereitung eines Datenträgers zur Speicherung von Dateien, in der Praxis gehen dadurch allenfalls Verzeichnisstrukturen und Dateinamen verloren. Wer schon einmal versehentlich eine Speicherkarte formatiert und anschließend die Fotos wiederhergestellt hat, weiß das eigentlich auch. Doch sicheres Löschen ist aufwendig, vor allem kostet es viel Zeit – das lohnt sich für die paar Euro nicht, die man auf eBay für eine gebrauchte Festplatte bekommt. Und doch ist den Verkäufern offenkundig ein Taschengeld wichtiger als der Schutz ihrer intimsten Daten.

Erschreckt hat uns, wie viele Verkäufer nicht einmal versuchten, ihre Daten zu löschen: Ihnen scheint es völlig egal zu sein, wer sie bekommt und was damit passiert. Im bayerischen Fall wäre nicht einmal der unverantwortliche Verkäufer der Haupt-Leidtragende gewesen, sondern seine Freundin, deren Nacktbilder samt Kontaktdaten überall im Internet hätten landen können. Also bitte Mädels, hört endlich auf mit den Nacktfotos für Eure Kerle – sie können nachweislich nicht damit umgehen. Und Jungs, wenn Ihr das Geld wirklich so dringend braucht, als dass Ihr Eure Festplatten oder Smartphones verkaufen müsst, löscht sie wenigstens ordentlich! Wie das geht, steht gleich auf der nächsten Seite. *(mid@ct.de)* c't

Literatur

[1] Lutz Labs, Sofortmaßnahmen am Unfallort, Datenrettung von Festplatte, Flash-Speicher und Smartphone, c't 24/14, S. 150

Kriminelle hätten dank hochauflösender Scans von Ausweisen, Staatsbürgerschaftsurkunden, Sozialversicherungskarten und Meldenachweisen leichtes Spiel, falsche Ausweise oder digitale Identitäten zu generieren und so zum Schaden der realen Personen Betrügereien abzuziehen.