Datenrettung und digitale Spurensammlung

Notaufnahme

Alexander Geschonneck

Ob Festplattencrash oder versehentlich Delete-Taste gedrückt – sind wichtige Geschäftsdaten verschwunden, sitzen Unternehmen ganz schön in der Patsche. Die *iX*-Marktübersicht zeigt, welche Dienstleister bei der Datenrettung und der Suche nach digitalen Beweisen bei Sicherheitsvorfällen helfen.

Fast jeder Computeranwender hat es schon erlebt: Wenn man am wenigsten damit rechnet, sind plötzlich wichtige Daten verschwunden, Dateien lassen sich nicht öffnen, oder die Festplatte gibt noch einige beunruhigenden Geräusche von sich, ehe sie sich endgültig verabschiedet. (Kurioserweise hatte der Autor beim Verfassen dieses Artikels einen Festplattenschaden am Computer – ein Backup der wichtigsten Daten verhinderte glücklicherweise größere Katastrophen.)

Ursache des Datenverlustes ist in vielen Fällen die physikalische Beschädigung der Speichermedien, die durch Herstellungs- und Wartungsfehler, aber auch durch äußere Faktoren erfolgen kann. So sind etwa die empfindlichen mechanischen und elektronischen Bauteile einer Festplatte bei einem Brand im Rechenzentrum beziehungsweise Büroraum oder bei Hochwasser extremen, für den Datenträger schädlichen Temperatur- und Feuchtigkeitsschwankungen ausgesetzt.

Dennoch müssen die gespeicherten Informationen nicht zwangsläufig verloren sein: Ist der Datenträger nicht zu stark zerstört oder finden sich auf den Oberflächenbeschichtungen der einzelnen Medien noch Informationen (siehe [1]), besteht tatsächlich die Chance, einige Daten wiederherstellen zu lassen – Voraussetzung ist allerdings, dass man nicht versucht hat, auf wenig professionelle Art die Daten selbst zu retten. Mitunter können die Rettungsspezialisten nur unvollständige Dateien und Verzeichnisse wiederherstellen, aber in einigen Fällen reicht dem Anwender bereits die Rekonstruktion von Daten- und Textfragmenten.

Teure Nachlässigkeit

Welche Folgen der Verlust wichtiger Daten für ein Unternehmen haben kann, zeigt das Ergebnis einer Sicherheitsstudie der Zeitschrift Kes aus dem Jahr 2002 (s. Abb. 1): 16 Prozent der befragten Unternehmen befürchteten existenzgefährdende Auswirkungen (Konkurs, Unternehmensende, Bankrott) bei einem Totalverlust ihrer Daten. Auch wenn dies eventuell zu dramatisch gezeichnet scheint, so ist bemerkenswert, dass immerhin 46 Prozent der Unternehmen in einem solchen Fall mit Einbußen von über 1 000 000 Euro rechnen. Umso erstaunlicher ist es, dass es zahlreichen Unternehmen noch immer an Disaster-Recovery-Konzepten oder gar Backup-

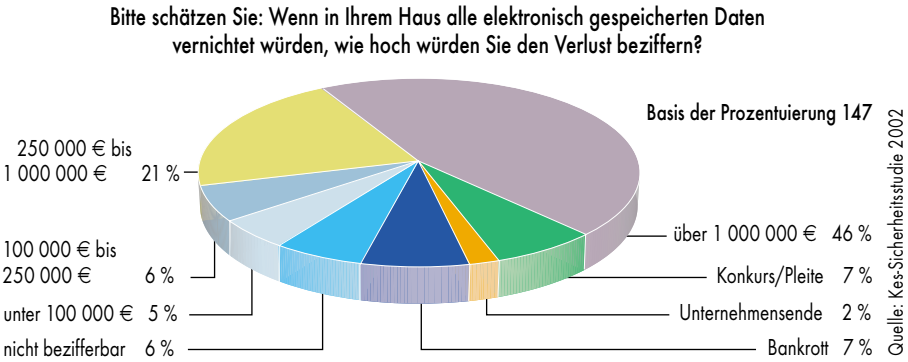
Lösungen mangelt, wie eine Umfrage unter 630 IT-Leitern aus verschiedenen Ländern belegt (www.aboutit.de/03/30/07.html).

Was aber tun, wenn das Kind in den Brunnen gefallen ist? Eine wachsende Anzahl von Spezialdienstleistern hat sich des Problems angenommen und versucht, zumindest einen Teil der Daten beziehungsweise Informationen des verzweifelten Kunden wiederherzustellen. In der vorliegenden Marktübersicht sind allerdings nur Firmen berücksichtigt, die ihre Dienste im deutschsprachigen Raum anbieten – alles andere wäre in besonders eiligen Fällen, oder falls Einsätze vor Ort erforderlich sind, kaum praktikabel.

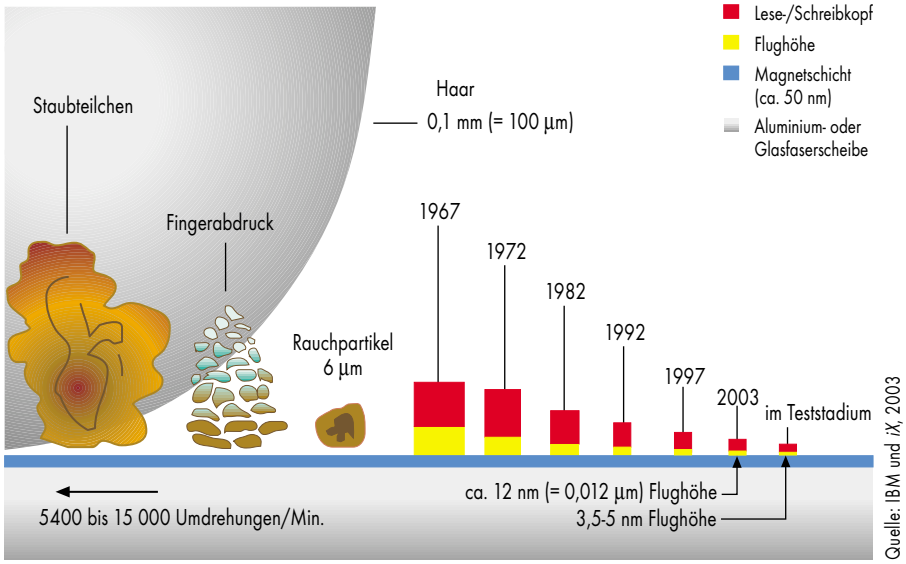
Preiswert sind die angebotenen Dienste freilich selten, benötigen die Retter in der Not doch enormes Spezialwissen und ein leistungsfähiges technisches Equipment. Wenn etwa an defekten Datenträgern Teile auszutauschen sind, muss ein Lagerbestand an Ersatzteilen für jedes Festplattenmodell (und sei es noch so alt) vorhanden sein. Auch sollte der Dienstleister über ausreichende und sichere Zwischenspeicherkapazität für die Analyse von Raid-Einheiten oder Backup-Tapes verfügen.

Ebenso wichtig sind gewisse infrastrukturelle Sicherheitsmaßnahmen zum Schutz der Datenträger und der wiederhergestellten Daten. Die Maßnahmen der Anbieter reichen vom einfachen Tresor über speziell gesicherte Räume bis hin zum kameraüberwachten Hochsicherheitstrakt. Hier kann der Kunde je nach Schutzbedarf seiner Daten den Dienstleister auswählen. Dasselbe gilt für die Rückgabe der wiederhergestellten Daten: Sensible Unternehmensdaten sollte man sich bevorzugt per Kurier – eventuell sogar auf einem passwortgeschützten Zieldatenträger – zurückbringen lassen, während für die privaten Urlaubsfotos das simple Versenden per Post oder eine Online-Übertragung genügen mag. Auf eine ausreichende Verschlüsselung sollte man allerdings auch in diesem Fall nicht verzichten.

Ein weiterer kritischer Punkt bei vertraulichen Daten ist der adäquate Schutz der Datenträger vor unbefugtem Zugriff beim Anbieter; hier sollte der Kunde einen Nachweis verlangen, dass die alten Datenträger nach erfolgreichen oder erfolglosen Rettungsversuchen fachmännisch und datenschutzgerecht entsorgt werden. Der Dienstleister sollte dazu fachkundig Auskunft geben können – insbesondere zum Thema Datenlöschen (siehe [1]), da viele der nicht mehr benötigten Speichermedien im Ersatzteillager des Dienstleisters landen.



Über 80 % der befragten Unternehmen rechnen im Fall eines totalen Datenverlustes mit drastischen finanziellen Konsequenzen bis hin zur Existenzgefährdung (Abb. 1).



Erschwerte Reinraumbedingungen: Mit zunehmender Speicherdichte der Festplatte und daraus resultierender Verringerung der Flughöhe des Schreib-/Lesekopfs wächst die Gefahr eines Headcrashes durch die mit bloßem Auge nicht mehr sichtbaren Schmutzpartikel (Abb. 2).

Gefahr durch Schmutzpartikel

Zur Ausstattung der meisten Anbieter gehört ein so genannter Reinraum; ein von der normalen Luftströmung abgegrenzter Bereich, in dem die Reinheit der enthaltenen Luft einer festgelegten Klasse entspricht. Er ist dann von Bedeutung, wenn für die Analyse beziehungsweise Reparatur des defekten Datenträgers das Gehäuse entfernt werden muss. Die Festplattenleseköpfe bewegen sich in der Regel mit einer Flughöhe von wenigen Nanometern über die Magnetschicht (s. Abb. 2). Ein mit bloßem Auge nicht mehr sichtbarerer Staub-

iX-TRACT

- Tritt ein Festplattenschaden auf, sollten auch IT-Fachleute keinesfalls an der Disk herumschrauben. Im schlimmsten Fall zerstört man dabei noch mehr Daten.
- Vor Beauftragung eines Datenrettungsunternehmens lohnt sich das Einholen einer Rettungsprognose. So erhält man frühzeitig Klarheit über Kosten und rettbare Daten.
- Wichtiger als das Schielen aufs Budget ist, dass der Kunde für s eine Anforderungen den bestmöglichen Dienstleister findet.

MARKTÜBERSICHT DATENRETTUNGS- UND FORENSIK-DIENSTLEISTER

Dienstleister	Mail; Kunden-Hotline	URL	Angebotene Dienstleistungen: Datenrettung/ vor Ort/remote	System-rettung	Gerichtsverwertbare Beweisspurensicherung auf Daten-trägern/ vor Ort	aus anderen Quellen[1]/ vor Ort	Erstellung foren-sischer Gutachten	Aktive Unter-stützung bei Sicher-heitsvorfällen	Sichere Entsorgung alter Daten/ Datenträger
Attingo	office@system.at; +43/1 484 72 96	www.system.at	✓/✓/–	✓	z. T./z.T.	z. T./z.T.	–	✓	A
Avantage Datenrettung OHG	info@datenrettung24.de; 030/692 29 92	www.datenrettung-24.de	✓/✓/–	✓	–/–	–/–	–	–	A
Böhlendorf	recovery@boehlendorf.de; 01 75/643 68 34	www.boehlendorf.de	✓/✓/–	✓	✓/–	–/–	–	✓	B
CBL Data Recovery Technologies GmbH	clientservices@cbltech.de; 00 800/87 38 88 64	www.cbltech.de	✓/✓/–	✓	✓/✓	✓/✓	✓	✓	C
CompuClinic	call@compuclinic.de; 08 51/76 96	www.compuclinic.de	✓/–/–	✓	✓/✓	✓/✓	✓	✓	B
Computerzeit Kleinsorg & Kübel & Pferrer OHG	datenrettung@computerzeit.de; 02 21/95 32 230	www.computerzeit.de	✓/✓/–	✓	✓/✓	✓/✓	–	✓	A; C
Convar Deutschland	datenretter@datenretter.de; 08 00/02 66 827	www.datenretter.de	✓/✓/✓	✓	✓/✓	✓/✓	✓	✓	C; D
Crash PC Service GmbH	info@data-recovery.de; 030/694 42 24	www.data-recovery.de	✓/✓/–	✓	–/–	–/–	–	–	C
Datex D.S.M.	info@datexeuropa.com; –	www.datexeuropa.com	✓/k. A./k. A.	✓	–/–	–/–	–	k. A.	A; C
DN-Systems Enterprise Internet Solutions GmbH	emerg@dn-systems.de; 051 21/289 89-10	www.dn-systems.de	–	–	✓/✓	✓/✓	✓	✓	B; C; D
Eltron Joechen & Rausch OHG	info@eltron.de; 089/375 05 20	www.eltron.de	✓/k. A./k. A.	✓	✓/✓	✓/✓	–	✓	A
Ibas Deutschland GmbH	mail@datenrettung.de; 08 00/42 27 112	www.datenrettung.de	✓/–/–	✓	✓/✓	✓/✓	✓	✓	B; D
Integralis GmbH [2]	info@integralis.de; –	www.integralis.de	✓/–/–	–	✓/k. A.	✓/✓	✓	✓	C
Interfile Datenrettung und Service	post@interfile.de; 025 71/91 94 99-0	www.interfile.de	✓/k. A./k. A.	✓	–/–	–/–	–	–	C; D
ITK-Datenrettung	info@itk-datenrettung.de; 08 00/483 63 37	www.itk-datenrettung.de	✓/✓/✓	✓	✓/✓	✓/✓	✓	✓	A
itn World	info@itnworld.de; 01 78/809 27 37	www.dataspezialist.de	✓/✓/✓	✓	✓/✓	✓/✓	✓	✓	A; B; C
KPMG	de-integrityservices@kpmg.de; 02 21/20 73 53 14	www.kpmg.com	–	–	✓/✓	✓/✓	–	–	ja (keine weiteren Angaben)
Kroll Ontrack	info@krollontrack.de; 070 31/64 41 50	www.ontrack.de	✓/✓/✓	✓	✓/✓	✓/✓	✓	✓	A; B
Kuert Datenrettung Deutschland GmbH	datenrettung@datenambulanz.de; 02 34/923 30 96	www.datenambulanz.de	✓/✓/–	✓	✓/–	✓/✓	–	✓	B; D
Maintec IT Service	info@maintec.org; 08 00/62 48 32	www.festplattenrettung.de	✓/–/–	–	✓/–	✓/✓	✓	in Kürze	C
MOV EDV-Datenrettung	erwin@edv-datenrettung.de; 01 73/47 99 810	www.edv-datenrettung.de	✓/–/–	✓	✓/–	✓/–	✓	✓	C
MSS Media	sv_buero@kupfrian.de; 023 51/796 35	www.mss-media.com	✓/k. A./k. A.	✓	✓/✓	✓/✓	✓	✓	C; D
Multimedia Service SH GbR	info@kueste.de; 048 32/53 35	www.internetwerbeagentur.de	✓/✓/–	✓	–/–	✓/✓	–	k. A.	D
ReBits-A.Späth GbR	support@rebits.de; 099 73/50 06 83	www.rebits.de	✓/–/–	✓	✓/–	✓/✓	–	–	A; C
Vogon International GmbH	datenrettung@vogon.de; 089/32 35 03-0	www.vogon.de	✓/✓/✓	✓	✓/✓	✓/✓	✓	✓	C

A = Rückgabe an Kunde
B = Datenlöschen durch Überschreiben
C = Physikalische Zerstörung durch Shreddern, Einschmelzen etc.
D = Magnetische Zerstörung durch Degausser, Löschspulen etc.

[1] z. B. Logfiles, Applikationen
[2] Einige Dienstleistungen werden nur in UK durchgeführt.

oder Rauchpartikel kann nicht nur eine unschöne Furche in der Oberfläche dieser Schicht, sondern im schlimmsten Fall einen Headcrash verursachen. Um das zu vermeiden, arbeiten die Datenrettungsexperten in aller Regel in einem Reinraum der Klasse 100. Das heißt, dass in Räumen dieser Klassifizierung in einem Kubikfuß Luft (ca. 28 l) maximal 100 Staubpartikel erlaubt sind. Zum Vergleich: Normale Umgebungsluft ist circa 10 000-mal unreiner.

Erreicht wird dieser definierte Zustand durch spezielle Isolier-, Filter- und Absaugvorrichtungen. Für die Spezialisten, die hier arbeiten, ist das Tragen von Schutzkleidung erforderlich. Ebenso wichtig ist bei Arbeiten und Messungen an den elektronischen Laufwerksbauteilen der Schutz vor elektrostatischen Entladungen in diesen Räumen, der durch zusätzliche technische Einrichtungen gewährleistet sein muss.

Hat man einen Anbieter ausgewählt, steht den Rettungsversuchen nichts mehr im Wege. Zunächst führen die Experten eine – teilweise kostenlose oder bei Auftragserteilung verrechenbare – Analyse durch, die dem Kunden zeigt, ob dem Datenträger überhaupt noch Informationen zu „entlocken“ sind. Hier gibt es unterschiedliche Verfahren: Ist die Festplatte zum Beispiel nicht lauffähig, schaut man mit einer Endoskopkamera über ein luftdicht

Sichere, für Unbefugte unzugängliche Lagerung	Rückgabe wiederhergestellter Daten (online/offline), ggfs. Sicherheitsmaßnahmen	Laborausstattung		Externe Vergabe	
		Reinraumlabor		der Datenrettung	
		vorhanden	ist zertifiziert	generell	bei physisch defekten Medien
gesicherter Raum	verschlüsselte Übertragung (SSL)	bei Partner	US-Federal-Standard 209 Klasse 10	–	z. T.
Tresor	Passwortschutz auf Zieldatenträger	✓	–	–	–
Tresor	keine Online-Übertragung; auf Wunsch werden Daten gebracht	–		–	z. T.
Sicherheitsschleuse, Alarmanlage, Security-Personal	verschlüsselte Übertragung (VPN)	✓	US-Fed-St 209 Klasse 100, 1000	–	–
Tresor	verschlüsselte Übertragung	✓	US-Fed-St 209	–	–
Gebäude mit Stahlgitter gesichert, (anonymisierte) Datenträger unter Verschluss	Datenträger kann zurückgebracht werden (Kurier oder selbst)	–		–	z. T.
Sicherheitsbereich, Tresor in unterirdischem Bunker	verschiedene Sicherheitslevels (Kurier, Verschlüsselung, Passwortschutz auf Zieldatenträger)	✓	ISO 14644-1, US-Fed-St 209 Klasse 1000, EG-GMP	–	–
Tresor	Passwortschutz auf Zieldatenträger	✓	–	–	bei Engpässen
verschlossene Aufbewahrung	keine Online-Übertragung	✓	nein, aber Partikelkontrolle	–	–
vergitterter Laborbereich, Zutrittskontrolle	keine Online-Übertragung; versiegeltes Paket zur Abholung	in Kürze		–	✓
Tresor	keine Online-Übertragung	✓	–	–	–
Tresor, zugangsgesicherte Labore	Online-Übertragung nur auf Wunsch; per Kurier	✓	US-Federal-Standard 209 Klasse 100	–	–
Sicherh.bereich, Zutrittskontrolle	k. A.	–		–	z. T.
alarmgesicherter fensterloser Raum, feuer- und wasserfest	verschlüsselte Übertragung (PGP, VPN); persönliche Übergabe; per Kurier	bei Partner	✓ (keine weitere Angabe)	✓	✓
Tresor	per Postpaket	✓	✓ (keine weitere Angabe)	–	–
gesicherter Raum, Zutrittskontrolle, verschließbarer Metallschrank	verschlüsselte Übertragung (VPN); per Post	bei Partner	ISO 14644-1	–	wenn Reinraum erforderlich
ja (keine weiteren Angaben)	ja (keine weiteren Angaben)	–		–	–
alarmgesichertes Labor, Tresor	keine Online-Übertragung; Medium nach Wahl per Kurier	✓	nein, aber entspricht Reinraum-Norm Klasse 100	–	–
gesicherter Raum	keine Online-Übertragung; Holen und Bringen durch Kurier	✓	–	–	–
Sicherheitsbereich mit Zutrittskontrolle und Videoüberwachung	keine Online-Übertragung; Einschreiben m. Rückschein	✓	US-Federal-Standard 209	–	–
ja (keine weiteren Angaben)	keine Online-Übertragung; per Post	✓	–	–	–
Auslagerung in Banktresor	keine Online-Übertragung; per Kurier	✓	–	–	–
–	Einschreiben m. R.; bis zum Eintreffen Kopieaufbewahrung	–		–	–
gesicherter Raum, feuerfester Tresor	Zusendung auf Leihfestplatten; CD per Kurier	✓	Zertifizierung für 2004 in Vorbereitung	–	z. T.
Sicherheitsbereich mit Zutrittskontrolle, Tresor	ja (keine weiteren Angaben)	✓	✓ (keine weitere Angabe)	–	–

✓ ja/vorhanden – nein/nicht vorhanden
k. A. = keine Angabe z. T. = zum Teil

Tabelle beruht ausschließlich auf Angaben der Anbieter

versiegeltes Diagnoseloch in das Innere der Platte, um nach sichtbaren Schäden und Verschmutzungen zu suchen. Des Weiteren werden die elektronischen Bauteile auf den Controllerplatinen einem Funktionstest unterzogen.

Bei vielen Datenträgern kann man über spezielle Diagnosemodi auf die Firmware zugreifen und einzelne Statusinformationen auslesen. Weist der Datenträger einen Wasser- oder Brandschaden auf, fallen diese Diagnosemöglichkeiten aber in der Regel aus. Einige wenige Anbieter versprechen für ihre Rettungsprognose eine exakte Auflistung derjenigen Dateien, die sie rekonstruieren können. Der Kunde kann anhand der Rettungsprognose einschätzen, ob die Kosten in einem wirtschaftlichen Verhältnis zum Wert der zu rettenden Daten stehen.

Nach der Beauftragung durch den Kunden erfolgt die eigentliche Wiederherstellung. Dazu erstellt der Fachmann Festplatten-Images durch bitweises Kopieren der Daten. Kann man durch leichte Korrekturen der Leseköpfe oder durch das Austauschen von elektronischen Bauteilen die Festplatte wieder zum Laufen bringen, genügt für das Kopieren die normale Festplattenschnittstelle.

Aufwendige Suchspiele

Ist das nicht möglich, müssen in einem wesentlich aufwendigeren Verfahren die einzelnen Magnetscheiben der Festplatte herausgenommen und gesondert ausgelesen werden. Im weiteren Verlauf versuchen die Datenretter, aus dem so erstellten Image die eventuell noch vorhandenen Dateien oder Verzeichnisse auszulesen beziehungsweise wiederherzustellen. Kann man auf diese Weise keine vollständigen Dateien retten, muss man die relevanten Daten durch Suche nach Zeichenketten aufspüren. Verständlicherweise lassen sich die Datenretter nur ungerne in die Karten schauen und halten die Details ihrer Methoden und Werkzeuge – die teilweise selbst entwickelt sind – geheim.

Normalerweise erlischt bei den beschriebenen Tätigkeiten die Gewährleis-

Verhalten bei Festplattenschäden

– Ruhe bewahren.

– Rechner herunterfahren beziehungsweise externe Festplatte sofort ausschalten.

– Festplatte auf keinen Fall selbst öffnen.

– Datenrettungsunternehmen kontaktieren, nach Möglichkeit Antworten auf folgende Fragen bereithalten:

- Wie ist das Problem entstanden und wie äußert sich der Fehler?
- Welche logische Struktur hat der Datenträger: Partitionierung, Dateisystem, Datenmengen?
- Beschreibung der wichtigen Unterverzeichnisse, Dateinamen, Dateitypen und -größen?
- Welche Versuche wurden bereits unternommen, um das Problem zu analysieren oder die Daten zu retten?

Auf den Webseiten der Anbieter finden sich häufig solche Fragebögen oder Stichwortlisten. Es vereinfacht den Ablauf, wenn man bei Anruf eines Datenretters die wichtigsten Informationen schon bereithält.

MARKTÜBERSICHT DATENRETTUNGS- UND FORENSIK-DIENSTLEISTER

Dienstleister	Externe Vergabe bei seltenen Dateisystemen/der forensischen Duplikation/ der Beweisspurensammlung, -bewertung	in anderen Fällen	Unterstützte Dateisysteme	Unterstützte Betriebssysteme	Unterstützte Datenträger/ Speichermedien	Preisgestaltung Festpreis/ nach Datenvolumen/ nach Aufwand/ nur bei Erfolg/ Rettungsprognose
Attingo	–/–/–		1, 2, 4, 6, 10, 11	18, 19, 21, 22	36–41, 46 weitere: DAT	–/✓/✓/✓/kostenpflichtig
Avantage Datenrettung OHG	–/–/–		1–17	18–34	35–48	✓/–/–/✓[3]/kostenpflichtig
Böhlendorf	✓/✓/z. T.	wenn Reinraum erforderlich	1–7	18, 19	35–47	✓/✓/✓/✓/kostenpflichtig
CBL Data Recovery Technologies GmbH	–/–/–		1–17	18–34	35–48	–/–/✓/✓/kostenlos
CompuClinic	✓/–/–		1, 2, 4–7, 9–12	18, 19, 21–23, 25, 26, 28	36, 38–40, 45, 46	Festpreisbereiche/–/ –/–/kostenpflichtig
Computerzeit Kleinsorg & Kübel & Pferrer OHG	–/–/✓	wenn Reinraum erforderlich	1–3, 5, 6, 11–14, 17	18, 19, 23, 28–31	35–46	✓/–/✓/–/kostenpflichtig
Convar Deutschland	–/–/–		1–17	18–34	35–48	–/–/✓/✓/kostenpflichtig
Crash PC Service GmbH	–/–/–		1–12	18–34	35–48	–/–/✓/✓/kostenlos
Datex D.S.M.	–/–/–		1, 2, 3, 11, 12	18, 19, 21–23, 28, 30, 31, 33	36	Festpreisbereiche/–/ –/✓/kostenpflichtig
DN-Systems Enterprise Internet Solutions GmbH	–/–/–		1–17, weitere: Veritas	18–34, weitere: Reliant Unix, SCO ODT-Server, NextStep	36, 38, 40, 43, 47, 48, weitere: HD MFM, DAT	–/–/✓/–/kostenpflichtig
Eltron Joechen & Rausch OHG	–/✓/–	bei Handys, PDAs	1–17	18–34	35–46	–/–/✓/✓[3]/kostenpflichtig
Ibas Deutschland GmbH	–/–/–		1–17	18–34	35–48	–/–/✓/–/kostenpflichtig[4]
Integralis GmbH [2]	z. T./z. T./z. T.		1–12, 14–17	18–25, 28, 30, 31, 34	35–46, weitere: DAT	–/✓/✓/–/kostenpflichtig
Interfile Datenrettung und Service	✓/✓/✓		1–6	18, 19, 21–23	35–48	✓/✓/✓/✓/kostenlos
ITK-Datenrettung	–/✓/✓		1–6, 11–15	18–24, 27–30	35–48	✓/✓/✓/✓/kostenpflichtig
itn World	–/✓/✓		1–17	18–34	35–48	✓/–/z. T./z. T./kostenlos
KPMG	–/–/–		1–17	18–34	35–48	–/z. T./✓/–/je nach Fall
Kroll Ontrack	–/–/–		1–17, weitere	18–34, weitere	35–48	–/–/–/–/je nach Fall
Kuert Datenrettung GmbH	–/–/✓		1–17	18–33	35–48	–/–/✓/✓/kostenpflichtig[4]
Maintec IT Service	–/–/–		1–6, 10–12	18, 19, 21–23, 28	35–46	✓/–/✓/✓/kostenpflichtig
MOV EDV-Datenrettung	–/–/–		1–17	18–34	35–48	✓/–/✓/–/kostenpflichtig
MSS Media	–/–/–		1–14	18–23, 26, 28–30	35–47	✓/–/✓/–/kostenpflichtig
Multimedia Service SH GbR	keine Annahme/ –/–		1–7	18	36–42, 44, 46	✓/–/✓/✓/kostenlos
ReBits-A.Späth GbR	–/–/–	wenn Engpass wegen fehlender Ersatzteile	1–11, 14–17	18–27, 30–34	36, 38, 40–42, 46, weitere: HD S-ATA, IBM Microdrive, PCMCIA	✓/–/✓/✓/kostenpflichtig
Vogon International GmbH	–/–/–		1–17	18–34	35–48	✓/–/✓/–/kostenpflichtig

Dateisysteme: **1** = FAT* **2** = NTFS **3** = komprimierte Dateisysteme **4** = ext2/3 **5** = HPFS **6** = HFS/HFS+ **7** = UFS **8** = XFS **9** = JFS **10** = ReiserFS
Betriebssysteme: **18** = Win* **19** = Linux **20** = BSD **21** = Mac OS < 9 **22** = Mac OS X **23** = OS/2 **24** = Solaris **25** = HP-UX **26** = AIX **27** = Irix
Speichermedien: **35** = MO **36** = HD (SCSI, EISA, IDE) **37** = USB-Massenspeicher **38** = Flash-Medien **39** = CD/DVD **40** = Floppy **41** = CompactFlash **42** = SM/CD **43** = DLT **44** = andere Tapes
[1] z.B. Logfiles, Applikationen [2] einige Dienstleistungen werden nur in UK durchgeführt [3] außer Diagnosekosten [4] Anrechnung bei Datenrettung ✓ ja / vorhanden – nein/nicht vorhanden

tung des Festplattenherstellers. Einige Hersteller bieten dennoch einen Ersatz im Rahmen der normalen Garantieleistungen an, wenn der Kunde den Nachweis erbringen kann, dass er ein professionelles Datenrettungslabor beauftragt hat. Eine Anfrage beim Datenretter schafft hier Klarheit, im Zweifelsfall hilft ein Blick auf die Webseiten der Hersteller von Datenträgern.

Rettung von speziellen Daten

Ein weiterer Bereich, bei dem oft die technischen und analytischen Fähigkeiten der Datenrettungsanbieter zum Einsatz kommen, ist die Beweismittelsicherung im Rahmen so genannter forensischer Ermittlungen, das heißt im Zusammenhang mit straf- und zivilrechtlichen Verfahren. Forensische Ermittlungen nach einem Systemeinbruch oder einem anderem Sicherheitsvorfall haben in der Regel die folgenden Ziele: das Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch oder der Straftat geführt haben könnte, die Ermittlung des entstandenen Schadens, die Identifikation des Angreifers und die Sicherung der Beweise für weitere juristische Schritte.

Als „typische“ computerbezogene Delikte sind neben Hackereinbrüchen etwa das Erstellen, Speichern und Verbreiten von kinderpornografischem Material oder illegaler Kopien von urheberrechtlich geschützten Inhalten zu nennen. Eine weitere Kategorie ist der so genannte Geheimnisverrat beziehungsweise die Wirtschaftsspionage. Analysieren muss man aber auch die Datenträger eines Tatverdächtigen aus dem „klassischen“ Kriminalitätsumfeld, wenn sein PC in irgendeiner Form an der Planung oder Durchführung des Vergehens beteiligt war.

Die forensische Duplikation sichergestellter Speichermedien hat sich quasi zu einem Standardvorgang bei der Ermittlung im Umfeld der Computerkriminalität entwickelt. Ein forensisches Duplikat ist letztendlich lediglich das Image eines Datenträgers, das bitweise als 1:1-Kopie erzeugt wurde. Dabei überträgt man – ähnlich wie bei der Datenrettung – unabhängig von den logischen Laufwerkszuordnungen den gesamten physischen Datenträgerinhalt auf ein zweites Medium [2]. In diesem Festplatten-Image können Experten nach verdächtigen Spuren und Beweisen für illegales Handeln suchen und bei Bedarf darüber ein Gutachten anfertigen.

Grundsätzlich suchen Ermittler nach Timestamps der Dateien und Verzeichnisse auf dem „verdächtigen“ Daten-

Sonstiges Express-Service	Abholung von Datenträgern	Ereichbarkeit der Hotline rund um die Uhr (24/7)	Besonderheiten/weitere Leistungen
gegen Aufpreis	gegen Aufpreis	–	Reparatur korrupter Dateien (MS Office, Datenbanken); Öffnen von passwortgeschützten Dokumenten
gegen Aufpreis	gegen Aufpreis	✓	
gegen Aufpreis	ohne Aufpreis	✓	Reparatur korrupter Dateien (MS Office, Datenbanken)
gegen Aufpreis	gegen Aufpreis	✓	
gegen Aufpreis	gegen Aufpreis	–	Passwort-Beseitigung bei IDE-Festplatten und Software
gegen Aufpreis	gegen Aufpreis	für registrierte Kunden	
generell Express	gegen Aufpreis	✓	Online-Informationssystem m. automatis. Statusabfragen etc.
gegen Aufpreis	gegen Aufpreis	✓	
–	gegen Aufpreis	–	Erhalt der Festplattengarantie (nicht alle Hersteller)
gegen Aufpreis	gegen Aufpreis	–	Patternanalyse mit Fremdsprachen, Forensic Accounting
gegen Aufpreis	gegen Aufpreis	✓	Gutachten für elektronische Schäden
gegen Aufpreis	gegen Aufpreis	✓	
gegen Aufpreis	gegen Aufpreis	–	
gegen Aufpreis	gegen Aufpreis	✓	Reparatur korrupter Dateien (ZIP, MS Office, Datenbanken)
gegen Aufpreis	gegen Aufpreis	✓	Reparatur korrupter Dateien und Datenbanken
gegen Aufpreis	gegen Aufpreis	✓	Datenkonvertierung
je nach Fall	gegen Aufpreis	–	Betrugsermittlung
gegen Aufpreis	gegen Aufpreis	✓	File-Listing aller rekonstruierbaren Daten
gegen Aufpreis	ohne Aufpreis	✓	
gegen Aufpreis	ohne Aufpreis	✓	Datenschutzzertifizierung in Vorbereitung
gegen Aufpreis	gegen Aufpreis	✓	Datenschutzzertifizierung in Vorbereitung
gegen Aufpreis	ohne Aufpreis	✓	Datenschutzzertifizierung vorhanden
gegen Aufpreis	gegen Aufpreis	✓	
–	gegen Aufpreis	–	Datenschutzzertifizierung in Vorbereitung; File-Listing aller rekonstruierbaren Daten
gegen Aufpreis	gegen Aufpreis	–	

11 = RAID-Systeme **12** = Netware **13** = Banyan Vines **14** = Solaris FFS **15** = OpenBSD FFS **16** = BSDi **17** = FFS
28 = Novel Netware **29** = Banyan Vines **30** = Unixware **31** = VMS **32** = OS390 **33** = OS400 **34** = Tru64
45 = LS 120 **46** = Zip/Jaz **47** = PDA **48** = Handys
k. A.= keine Angabe z. T. = zum Teil

Tabelle beruht ausschließlich auf Angaben der Anbieter

träger, nach eventuell trojanisierten Systemprogrammen, versteckten Dateien und Verzeichnissen sowie nach weiteren auffälligen Dateien, Sockets und Prozessen. Hier genügt häufig ein einziger Ansatzpunkt, um eine Spur von Tat oder Täter zu finden.

Für das Erstellen des Festplatten-Images existieren verschiedene Verfahren, deren Auswahl unter anderem von den lokalen Gegebenheiten am Einsatzort abhängt;

– die Ermittler entfernen die Festplatte aus dem verdächtigen System und schließen sie an ihr Analysesystem an;
– die Ermittler schließen eine zusätzliche „saubere“ Festplatte an das verdächtige System an;
– sie übertragen die kopierten Daten über ein (geschütztes) Netzwerk auf ihr Analysesystem.

Um das versehentliche Überschreiben der zu untersuchenden Disk zu verhindern, schließt man in der Regel zusätzlich so genannte Write-Blocker an.

Die Auswertung von Daten eines forensischen Festplattenduplikats ist mitunter sehr zeitaufwendig. Die Entscheidung, ob ein solches Duplikat angefertigt werden sollte, hängt im Wesentlichen davon ab, ob eine straf- oder zivilrechtliche Verfolgung in Betracht kommt und ob Dateien zu Beweiszwecken wiederherzustellen sind. Ein weiterer Faktor ist der potenzielle Produktionsausfall durch die Analyse, da das betroffene System während der Duplikation offline ist. Für eine Duplikation hingegen spricht es, wenn der unbenutzte Speicherbereich (unallozierte Bereiche, File-Slack, Partition Gap et cetera) des Datenträgers analysiert werden muss.

Eine forensische Ermittlung ist allerdings mehr als das Kopieren von Festplatten und das Auflisten der dort gefun-

Relevante Fragen für die forensische Ermittlung

- War zum Durchführen der strafbaren Handlung physischer Zugang zum PC nötig?
- Welche Personen hatten außer dem Verdächtigen noch Zugang zu dem fraglichen Computer?
- War auf dem PC ein Cronjob oder Scheduler aktiv, der die verdächtige Handlung ohne Anwesenheit des Tatverdächtigen durchführen konnte?
- Existieren weitere Beweise, die die Auswertung der digitalen Spuren bestätigen oder ihr widersprechen?
- Über welche Computerkenntnisse verfügt der Tatverdächtige oder seine potenziellen Mittäter wirklich, beziehungsweise welche Kenntnisse sind für die Tatdurchführung nötig?
- Ist die Hardware transportabel, oder kann der Tatverdächtige seinen Standort durch die Verwendung mehrerer Computer verschleiern?
- Könnte ein Tatverdächtiger den Angriffscode, verräterische Dokumente, E-Mails et cetera geschrieben haben (dem Stil, Vokabular oder bestimmten Redewendungen nach zu urteilen)?
- Können vom Tatverdächtigen besuchte Webseiten mit dem Sachverhalt in Verbindung gebracht werden?
- Finden sich Hinweise auf E-Mails oder Chat-Rooms beziehungsweise IRC-Channels, durch die eventuelle Mittäter beziehungsweise Mitwisser oder weitere Angriffsziele identifiziert werden könnten?

denen Dateien. Es gehört ebenso dazu, flüchtige Informationen am verdächtigen System vor Ort zu erfassen und später zu analysieren. Dazu müssen die Experten innerhalb kürzester Zeit so viele kurzlebige Informationen wie möglich sammeln, ohne überall ihre eigenen „Fingerabdrücke“ zu hinterlassen. Schließlich handelt es sich um wichtige Statusdaten, die sowohl nach dem Herunterfahren als auch nach dem Steckerziehen am Rechner nicht mehr verfügbar sind [2]. Egal für welche der beiden Optionen man sich entscheidet, der Status des Systems wird auf jeden Fall während der Untersuchung verändert.

Für die Sammlung dieser flüchtigen Informationen sollte man unter keinen Umständen die Systembefehle verwenden. Zum einen, weil es sich unter Umständen um trojanisierte Programme handelt, die entweder bestimmte Informationen verbergen oder auch Schadfunktionen aktivieren können. Zum anderen würde die Verwendung der lokalen Kommandos deren Zeitstempel des letzten Aufrufs verändern. Daher sollte man ausschließlich mit eigenen, sicheren und aus vertrauenswürdiger Quelle stammenden Dateien arbeiten. Unabhängig davon, welche Tools und Verfahren (hier befindet sich ein Überblick: computer-forensik.rg/tools.html) zum Einsatz kommen, ist das Sammeln der folgenden Informationen erforderlich: Systemdatum und -uhrzeit (mit Abweichung von einer Referenzzeit), Liste der aktiven Prozesse, Netzverbindungen und der angemeldeten Benutzer, Inhalt von Cache, RAM, Swapfiles et cetera (siehe [3]). Sind diese Daten erfasst, kann man sich auf die Suche nach weiteren verdächtigen Spuren am System begeben.

Zusammenführung aller Fakten

Erst wenn die Experten die digitalen Beweise mit den „physischen“ in Verbindung bringen, lässt sich ein Bild vom möglichen Tathergang zeichnen. Eine abschließende Bewertung des gesamten Sachverhalts ohne die Würdigung des weiteren Umfelds ist nur selten sinnvoll. Für die Beurteilung der digitalen Spuren sind die im Kasten „Relevante Fragen …“ aufgeführten Punkte von Bedeutung.

Die abschließende Bewertung aller Fakten kann in Form eines forensischen Gutachtens erfolgen. Das lohnt sich insbesondere, wenn eine gerichtliche Verfolgung des Vorfalls angestrebt wird. Bei der Erstellung eines Gutachtens ist allerdings Vorsicht geboten, denn nicht immer ist das, was möglich und wahrscheinlich ist, auch wirklich passiert. Seriöse Gutachter zeichnen sich dadurch aus, dass sie in mehrdeutigen Fällen nur die Fakten darstellen und Vermutungen als solche kennzeichnen.

Viele der befragten Datenrettungsunternehmen bieten diese und andere Dienstleistungen aus dem forensischen Umfeld an, allerdings in unterschiedlichem Umfang. Nicht alle führen beispielsweise Untersuchungen vor Ort durch. Andere helfen zwar bei der Beweisspurensammlung, erstellen aber kein Gutachten. Hier muss der Kunde je nach Sicherheitsvorfall abwägen, welche Hilfe er genau benötigt.

Der letzte Punkt schließlich betrifft die eingesetzten Formate und Speichermedien: Viele Unternehmen haben noch den ein oder anderen hochbetagten Rechner in Betrieb. Nicht alle Dienstleister unterstützen jedoch ältere oder auch seltene Betriebs- oder Dateisysteme. Ein Blick auf die Website hilft nur bedingt weiter, denn unter den beispielhaft aufgeführten Formaten finden sich eher die Standardsysteme als die Exoten. In speziellen Fällen hilft nur das Nachfragen. Dasselbe gilt für Datenträger: Noch sind Medien wie Handys und PDAs nicht alt genug, als dass schon alle Dienstleister mit der Rettung der darauf befindlichen Daten vertraut wären.

Fazit

Mit ausgefeilten technischen Verfahren ist bei der Datenrettung sowie bei forensischen Ermittlungen mehr möglich, als man gemeinhin annimmt. Billig sind solche Dienstleistungen in aller Regel jedoch nicht. Ein vernünftiges Backup-Konzept ist das zwar auch nicht, im Ernstfall dauert der Ausfall der Systeme aber weniger lange, der Produktivitätsverlust ist somit geringer, und weniger nervenaufreibend ist ein Backup-Recovery obendrein.

Tritt der schlimmste Fall dennoch ein, lohnt es sich in jedem Fall, die von allen Unternehmen angebotene Rettungsprognose wahrzunehmen. Man erhält so Klarheit über Kosten, rettbare Daten und gegebenenfalls Rentabilität des Vorgangs. Bei wichtigen Geschäftsdaten sollten die Kosten jedoch nicht im Vordergrund stehen: Ausschlaggebend ist letzten Endes, den bestmöglichen Dienstleister für die eigenen Anforderungen zu finden. (ur)

ALEXANDER GESCHONNECK

ist leitender Sicherheitsberater bei der HiSolutions AG in Berlin, sowie Autor des Ende Januar im dpunkt-Verlag erscheinenden Buches „Computer Forensik – Systemeinbrüche erkennen, ermitteln und aufklären“.

Literatur

[1] Lukas Grunwald; Datenentsorgung; Blitzblank; Sicheres Löschen von Speichermedien; *iX* 5/2003, S. 72

[2] Lukas Grunwald; Digitale Forensik; Ausgrabungen; Beweissicherung bei Computerdelikten; *iX* 10/2002, S. 100

[3] Alexander Geschonneck; Computer-Forensik – Systemeinbrüche erkennen, ermitteln, aufklären; dpunkt-Verlag 2004