Merkblatt: Datenrettung unter Ubuntu

Prävention und Realisation, Stand: 04/2014

Wichtiger Hinweis: die nachfolgenden Informationen empfehlen wir ausschließlich für versierte Anwender, die wissen, was Sie tun. Wir übernehmen per se keine Haftung für Selbstversuche und dadurch verursachte direkte oder indirekte materielle und immaterielle Schäden. Grundsätzlich raten wir nur zu einem Selbstversuch, wenn der Verlust der Daten in Kauf genommen werden kann.

Im alltäglichen Stress kann es leicht geschehen, dass Dateien gelöscht werden, die eigentlich nicht zur Löschung vorgesehen waren. Wenn dies geschieht, können aber verschiedene Maßnahmen ergriffen werden, um die Daten wieder zu retten. Es ist in jedem Betriebssystem sinnvoll, die Wege zur Datenrettung bereits zu kennen, bevor der Notfall eintrifft. Wer nach der Löschung der Daten erst beginnt, nach den Rettungswegen zu suchen, könnte unbeabsichtigt die gelöschten Dateien endgültig zerstören. Am leichtesten ist die Datenrettung, wenn alle hierzu erforderlichen Programme bereits auf der Festplatte installiert sind. Doch es gibt auch genügend Wege, die gelöschten Daten vor einer Überschreibung zu schützen, wenn zuvor noch Installationen notwendig sein sollten. Der wichtigste Griff nach einer versehentlichen Datenrettung ist die Tastenkombination Alt + Druck + U, welche sofort sämtliche Schreibzugriffe für die aktuell genutzte Partition sperrt. Auf diese Weise wird verhindert, dass neu gespeicherte Daten die zu rettende Datei teilweise überschreiben.

Schutz vor Datenverlust unter Ubuntu

Damit es erst gar nicht notwendig wird, Daten zu retten, sollte stets mit Sorgfalt gearbeitet werden. Beim Löschen von Daten ist der Papierkorb eine sinnvolle Unterstützung. Dateien, die hierher verschoben werden, können zwar nicht mehr genutzt werden, sind aber noch nicht zum Überschreiben freigegeben. Falls eine Datei gelöscht wird, die an anderer Stelle doch noch benötigt wird, kann sie ohne großen Aufwand wieder hergestellt werden. Gerade wenn im Laufe einer Aufräumaktion viel Datenschrott beseitigt werden soll, kann mit dieser Maßnahme ein versehentliches Löschen verhindert werden. Zu leicht kann es geschehen, dass unbemerkt zwei Dateien statt nur einer markiert wurden. Auch beim Leeren des Papierkorbes sollte noch einmal geprüft werden, ob die hier liegenden Dateien wirklich zu

löschen sind. Wenn dann doch einmal eine Datei verschwindet, kann die Datensicherung viel Ärger ersparen. Regelmäßige Sicherungskopien der gesamten Festplatte erlauben eine Herstellung der Daten zu einem bestimmten Zeitpunkt. Je häufiger die Kopien angelegt werden, desto aktueller ist auch die mögliche Datenrettung. Das Intervall für das Back-up sollte dem individuellen Datenvolumen angepasst sein. Wer viele und wichtige Daten über sein System verwalten muss oder zum Beispiel an zahlreichen Projekten arbeitet, sollte drei Sicherungskopien anlegen. Die eine sollte täglich aktualisiert werden, die nächste wöchentlich und die letzte kann dann im monatlichen Abstand erneuert werden. Auf diese Weise können auch dann Daten gerettet werden, wenn die versehentliche Löschung erst nach dem Erstellen des nächsten Back-ups auffällt.

Das System auf mögliche Rettungsversuche vorbereiten

Für den Fall, dass eine Datenrettung notwendig wird, sollte das System bereits entsprechend eingerichtet werden. Die Festplatte sollte zum Beispiel in zwei oder mehr Partitionen aufgeteilt werden. So kann die betroffene Partition mit der Tastenkombination Alt + Druck + U gesperrt werden, ohne das System vollständig abzuriegeln. In der zweiten Partition kann dann noch immer nach einem geeigneten Weg gesucht werden, um die Daten wiederherzustellen. Wer keine Partitionierung der Festplatte vorgenommen hat, sollte sich die notwendigen Rettungsprogramme mithilfe eines zweiten Rechners beschaffen. Die Installation des Rettungsprogrammes könnte sonst die Daten, die gerettet werden sollen, endgültig zerstören. Wer sich rechtzeitig auf den Fall vorbereiten möchte, sollte daher die entsprechenden Rettungsprogramme bereits betriebsbereit auf der Festplatte haben.

Die richtige Datenrettung für das Dateisystem

Nicht jede Methode der Datenrettung arbeitet auf jedem Dateisystem. Während lange Zeit unter Linux vor allem das System ext2 genutzt wurde, ist mit der Linux-Version 2.4.15 ein Journaling-System unter der Bezeichnung ext3 eingeführt worden. Das neuere System hat den Vorteil, dass es stabiler läuft als der Vorgänger. Im Falle eines Systemabsturzes bleiben die Metadaten unbeschädigt. Jedoch werden in diesem Dateisystem gelöschte Daten mit Nullen überschrieben. Dies kann nach einem Absturz die Fehlerquote senken, erschwert jedoch das Wiederherstellen versehentlich gelöschter Daten. Im Folgenden werden daher die Möglichkeiten der Datenrettung zunächst für das Dateisystem ext2 und später für ext3 und 4 getrennt voneinander behandelt.

Datenrettung mit e2undel

e2undel ist ein Datenrettungsprogramm, das auf einfache Weise die Rettung gelöschter Daten ermöglichen soll. Um dieses Programm zu nutzen, muss das betroffene Dateisystem zunächst ausgehängt werden. Vorsicht ist jedoch bei USB-Sticks angesagt. In der Regel werden diese Speichersticks nur mit Lesezugriff eingehängt. Alle zu speichernden Daten werden zunächst nur im Zwischenspeicher gelagert, um dann beim Aushängen auf den Datenträger geschrieben zu werden. Wurde auf dem USB-Stick eine Datei versehentlich gelöscht, könnte sie gerade durch das Aushängen endgültig zerstört werden. Das Programm e2undel sollte daher vor allem bei internen Speichern genutzt werden. Falls das Dateisystem noch fast frei ist und die gelöschte Datei weniger als 48 KB misst, kann im Einzelfall auch auf das Aushängen verzichtet werden. Bei genügend freiem Speicherplatz ist die Gefahr etwas geringer, dass wichtige Bestandteile der Datei während der Nutzung von e2undel überschrieben werden. Sinnvoller ist aber, unabhängig davon, an welcher Stelle die gelöschte Datei liegt, das Datenrettungsprogramm mithilfe einer Live-CD zu nutzen. Auf diese Weise kann selbst die Partition, auf der das Betriebssystem liegt, ohne Gefahr nach gelöschten Dateien durchsucht werden. Insgesamt kann gesagt werden, dass e2undel ein komfortables Programm ist, mit dem Daten sicher wiederhergestellt werden können. Hierfür muss es jedoch bereits installiert sein, bevor die Datei, die gerettet werden soll, gelöscht wurde.

Bereits vorinstalliert: debugfs

Das Paket e2fsprogs enthält unter Ubuntu das Programm debugfs bereits und kann daher im Notfall leicht genutzt werden. In diesem Programm kann mit dem Befehl open /dev/hda3 das betroffene Laufwerk angewählt werden. hda3 ist dabei durch den entsprechenden Laufwerksnamen zu ersetzen. Der Befehl lsdel zeigt dann alle gelöschten Dateien dieses Laufwerks an. Mithilfe des Löschdatums und der Dateigröße kann die richtige Datei leicht gefunden werden. Die in dieser Liste angegebene Inode-Nummer ist für die Datenrettung entscheidend. Der Befehl dump[Zieldatei] verschiebt die Datei mit der angegebenen Nummer in das gewählte Verzeichnis. Falls mehrere Dateien gerettet werden müssen, kann die Liste aller gelöschten Dateien auch in einer Textdatei ausgegeben werden. In dieser Datei werden dann alle Zeilen gelöscht, die korrekt vernichtete Daten benennen. Die übrigen Dateien werden mit einer Schleife an den Befehl dump gegeben. Die Dateien können auf diese Weise vollständig in ein zuvor erstelltes Verzeichnis verschoben werden. Die Dateinamen müssen nun jedoch von Hand wiederhergestellt werden, da die Dateien mit der zuvor ermittelten Inode-Nummer abgespeichert werden.

Daten nach Ausdrücken durchsuchen

Mit dem Befehl grep, der mit einem gleichnamigen Paket installiert ist, kann jeder Bereich des Dateisystems nach bestimmten Zeichenketten durchsucht werden. Diese Funktion kann auch zur Datenrettung genutzt werden. Wird etwa der Befehl grep -a -B200 -A600 “Doktorarbeit” /dev/hda3 >/tmp/recovered eingegeben, sucht das Programm zunächst nach der Zeichenkette Doktorarbeit. Die vorangestellten Zahlen B200 und A600 geben an, dass der Datenbereich von 200 Zeilen vor bis 600 Zeilen nach der gefundenen Zeichenkette relevant ist. Dieser Datenbereich wird dann im Zielordner, in diesem Fall /tmp/recovered, als Textdatei gespeichert. Die Angabe /dev/hda3 beschränkt in diesem Befehl die Suche auf das betroffene Laufwerk hda3. In der so gespeicherten Textdatei können die gelöschten Daten nun wieder herausgelesen werden. Wichtig ist, dass die Länge der gesuchten Datei bekannt sein muss. Auch muss ein Wort gefunden werden, welches möglichst nur in der gesuchten Datei genutzt wurde. Zur Rettung von Bilddateien oder anderen Daten eignet sich diese Methode nur bedingt. Die in der Textdatei gespeicherten Daten ließen sich bei Bedarf aber auch wieder in ein entsprechendes Format umwandeln. Wenn alle Daten gerettet sind, muss natürlich der Schreibschutz der betroffenen Partition wieder aufgehoben werden, um normal weiterarbeiten zu können. Erst dann kann die Datei wieder an ihren ursprünglichen Platz geschoben und dort gespeichert werden.

Datenrettung auf ext3

Da gelöschte Daten unter ext3 durch Nullen überschrieben werden, ist die Datenrettung hier nicht ganz einfach. Die meisten Programme, die unter ext2 laufen, werden hier nicht funktionieren, da die Daten grundsätzlich schon einmal überschrieben wurden. Sofern die Datei aber mindestens 48 KB groß war, besteht die Möglichkeit, zumindest einer teilweisen Wiederherstellung. Eine gute Möglichkeit stellt das Programm ext3rminator dar, welches unter der Live-Linux-Distribution grml zu finden ist. Der Rechner sollte mithilfe dieser Live-CD neu gestartet werden. Da diese Linux-Version nicht installiert werden muss, kann sie ohne Bedenken eingesetzt werden. Es sind keine Veränderungen im Dateisystem notwendig, daher ist grml ein häufig empfohlenes “Datenrettungstool”, welches nicht nur unter Ubuntu funktioniert. Neben den Standard-Programmen, die mit grml geliefert werden, können auch zahlreiche andere Programme gefunden werden. So zum Beispiel extundelete, ext3grep und viele mehr. All diese Programme arbeiten nach dem System des Befehls grep, der einzelne Datenfragmente kopieren kann. Zur Rettung von Texten oder schriftlichen Datenbankeinträgen sind die Programme sehr hilfreich. Die Datenfragmente müssen

allerdings anschließend manuell wieder zu den ursprünglichen Dateien im korrekten Format umgewandelt werden. Bei Grafiken oder Audiodateien wird es sehr schwierig die korrekten Datenfragmente zu identifizieren, um die Daten wieder lesen zu können.

Datenrettung bei defekter Festplatte

Auch wenn menschliche Fehler die häufigste Ursache für verlorene Daten sind, können manchmal auch Defekte dafür verantwortlich sein. Ein Stromausfall, der ein ordentliches Herunterfahren des Systems verhinderte, kann ebenso einen Datenverlust verursachen, wie eine Überspannung durch Blitzschlag. Auch ohne besonderen Grund kann der Lesekopf versagen und einen Crash verursachen. In all diesen Fällen muss Ruhe bewahrt werden. Ein allzu hastiger Blick auf die Festplatte, um den Schaden einzuschätzen, kann noch mehr Daten zerstören. In jedem Fall ist es wichtig, den Rechner abgeschaltet zu lassen, um herauszufinden, was genau geschehen ist. Wenn tatsächlich ein physischer Schaden vorliegt, können einfache Datenrettungsprogramme nicht mehr helfen. In diesem Fall muss ein Fachmann zunächst die physischen Komponenten der Festplatte behandeln, um auf die Daten zugreifen zu können. Ist die Platte dagegen äußerlich in Ordnung, kann versucht werden, das Dateisystem einzuhängen. Oftmals sind doch weniger Daten betroffen als anfangs vermutet. In diesem Fall können die Dateien mit einem Programm wie zum Beispiel Badblocks auf fehlerhafte Stellen kontrolliert und auf einen anderen Datenträger kopiert werden.

Nicht mehr einhängbare Partition

Wenn die Partition so stark beschädigt ist, dass sie sich nicht mehr richtig einhängen lässt, wird ein Programm wie zum Beispiel dd_rescue benötigt, um die Daten doch noch erreichen zu können. Um dieses Programm nutzen zu können, wird ein System benötigt, in welchem mindestens doppelt so viel Speicherplatz zur Verfügung steht, wie die betroffene Partition einnimmt. Dieser Platz sollte auf einer neuen, unbeschädigten Festplatte zur Verfügung stehen. Nachdem auf der zweiten Festplatte eine ausreichend große Partition eingehängt wurde, kann mit dem befehl dd_rescue [betroffene Partition] [geschaffene Partition]/image.dat ein Abbild der beschädigten Dateien geschaffen werden. Die nicht mehr lesbaren Stellen der beschädigten Partition werden von dd_rescue durch Nullen ersetzt. Auf diese Weise werden die noch erhaltenen Daten in einem exakten Spiegelbild gespeichert. Wenn ein besonders großer Schaden auf der Partition gefunden wird, kann das Programm unter Umständen nicht mehr weiterarbeiten. In diesem Fall kann der Befehl abgebrochen werden. Die übrigen Daten werden kopiert, indem der gleiche Befehl mit dem Zusatz -r

erneut aufgerufen wird. Die Zieldatei muss nun eine andere sein, dann wird dort die defekte Partition vom Ende her gespeichert. Ist die fehlerhafte Stelle erneut erreicht, stehen Anfang und Ende der Partition wieder zur Verfügung. Die noch fehlende Datenmenge kann nun berechnet und mit Nullen aufgefüllt werden, um wieder einen vollständigen Spiegel der Partition zu erhalten. Eine Sicherungskopie dieses Spiegels verhindert, dass die Daten bei einem fehlgeschlagenen Rettungsversuch doch noch verloren gehen. Der Befehl fsck.ext3 -p /mnt/image.dat kann dann die fehlerhaften Dateien reparieren und in einen lesbaren Zustand versetzen. Falls alles funktioniert hat, kann das Dateisystem nun wieder eingehängt und die Dateien geöffnet werden. Zur Sicherheit sollte zunächst nur ein Lesezugriff gewählt werden. Alle Dateien, die sich nun öffnen lassen, sollten umgehend in ein anderes, unbeschädigtes Dateisystem kopiert werden. Datenträger, die einen Defekt aufweisen, sollten nach der Rettung der Daten umgehend entsorgt werden, damit zukünftige Daten nicht durch weitere Defekte vernichtet werden.

Imprint

Informationen gemäß TMG:

Fuchs Media Solutions

Manuel Fuchs, B.A.

Schluchweg 4

D- 78166 Donaueschingen

Inhaltlich verantwortlich:

Manuel Fuchs, B.A., Anschrift (s.o.)

Tel. +49 (0) 771 / 1589439 (Mo-Fr 08.00 – 18.00 Uhr)

Email: info@it-service24.com

Web: http://www.it-service24.com/

UstID-Nummer: DE 230 97 77 50

Rechtsform: Einzelunternehmen