Gefahr beim Austausch von Festplatten

Eine Prüfung für ein führendes Finanzinstitut beweist, dass sich die Daten ausgefallener RAID-Disks aus einem aktiven Storage-System wiederherstellen lassen. Besser ist es, vor einer Übergabe an den Hersteller, Festplatten sicher zu löschen. Kroll Ontrack bietet dazu umfassende Services und Produkte.

In der Werbung der Hersteller hört sich alles so schön an: Durch den Einsatz eines RAID 6 Storage-Systems lassen sich die negativen Auswirkungen eines Festplattenausfalls wirksam bekämpfen. Denn durch den zweifachen Einsatz von Paritätsprüfungs-Einträgen auf allen RAID-Festplatten können sich im schlimmsten Fall zwei von vier Festplatten im RAID-Set dauerhaft abschalten, ohne dass dadurch das System als Ganzes gefährdet ist. Und im Rahmen der üblichen Wartungsverträge bietet der Hersteller einen unkomplizierten Austausch der ausgefallenen Festplatte. Nur: Was passiert dann eigentlich mit den verbliebenen Daten auf dieser Disk? Besteht hier nicht das Risiko, dass Unbefugte an unternehmensinterne Informationen kommen können?

Dass sich das gesamte RAID 6 beim Rebuild aufhängt und man danach ein komplett zerstörtes Storage-System zur Verfügung hat, ist leider recht häufig der Fall. Denn mit den Parity-Einträgen auf den verbleibenden funktionierenden Disks kann ein RAID 6 Rebuild gestartet werden. Ein Rebuild ist dabei nichts anderes, als eine Wiederherstellung der Daten aus den Parity-Informationen der intakten Festplatten. Ein einziger kleiner Lesefehler bei einer der verbliebenen Platten allerdings kann Grund sein, dass die Wiederherstellung des RAIDs fehlschlägt. Aber auch dass sich einzelne RAID-Festplatten überhitzen und dadurch ausfallen oder dass der verwendete RAID 6 Controller defekt ist und einen Ausfall eines oder mehrerer Platten überhaupt nicht anzeigt, bis das System komplett ausfällt, passiert ebenfalls leider viel zu häufig. Auch die Nutzung eines RAID 6 Systems schützt also nicht vollständig vor einem Datenverlust.

Vor einem Rebuild – also vor der Wiederherstellung des RAID 6 Systems inklusive aller Daten – muss zunächst die ausgefallene Festplatte durch eine neue ersetzt werden, weil ansonsten die RAID-Steuerungssoftware versucht, die vermutlich defekte Platte neu einzubinden. Nach einem Festplattenausfall muss die betroffene Disk aus dem RAID 6-Verbund also unbedingt entfernt und ausgetauscht werden.

Für diesen Fall bieten die Hersteller einen Plattenaustausch-Service als Teil des mit dem Kunden abgeschlossenen Wartungsvertrags an. Dazu sieht der RMA-Prozess (Return-Material-Authorization) entweder vor, dass der Kunde die ausgefallenen oder defekten Platten an den Hersteller zurücksendet oder dass ein Servicemitarbeiter die neue Disk einbaut und die alte mitnimmt. Den Verbleib einer defekten Platte beim Kunden sieht dieses Konzept meistens nicht vor. Wenn überhaupt, ist ein solcher Wunsch mit zusätzlichen Kosten für den Kunden verbunden. Bei der Rückgabe der alten ausgefallenen Festplatte an den Hersteller ist allerdings nicht sichergestellt, dass die darauf enthaltenen Daten dann später auch sicher gelöscht werden.

In der Konsequenz kann ein Unternehmen bei diesem Prozess niemals sicher sein, dass keine geschäftskritischen oder unternehmensinternen Informationen auf diesem Weg in fremde Hände gelangen. Die Gefahr eines ungewollten Datenlecks ist hier offensichtlich.

Lassen sich Daten aus RAID-Stripes auslesen?

Bei der Geschäftssparte eines führenden Finanzinstituts galt es deshalb zu prüfen, wie hoch die Gefahr eines unbeabsichtigten Datenlecks durch den Austausch von defekten Festplatten aus einem Storage-System eigentlich ist. Kernfrage dabei: Ist es möglich, aus einzelnen, aus einem RAID 6 System entnommenen Festplatten Daten so wiederherzustellen, dass Kriminelle verwertbare Informationen über einzelne Mitarbeiter oder gar Unternehmensinterna bekommen?

Zur Beantwortung dieser Frage wurde aus einem laufenden RAID-System eine aktive (und völlig intakte) Festplatte entnommen und umfangreichen forensischen Tests mit speziellen Softwarewerkzeugen im Kroll Ontrack Labor unterzogen.

Das Ergebnis war erschreckend: Den Kroll Ontrack Spezialisten war es tatsächlich gelungen aus den Stripe-Datenblöcken der einzelnen RAID-Festplatte viele verwertbare Informationen auszulesen und wiederherzustellen. Aufgrund der Stripe-Struktur eines RAIDs sind die größten Dateien immer maximal so groß wie die beim Aufsetzen des RAIDs festgelegte Stripe-Größe. In diesem Fall war die Stripe-Block-Größe auf 4 Kilobyte festgelegt. So waren auch in diesem Fall kleinere Dateien bis zu dieser Größe im vorhandenen NetApp RAID 6 System komplett vorhanden und vollständig lesbar. Aber auch größere Dateien, die nicht vollständig wiederhergestellt werden konnten, waren in vielen Fällen mit entsprechenden Viewern zu öffnen, nur das Layout der Dateien war entweder unvollständig oder nicht mehr vorhanden. Die reinen Informationen konnten problemlos gelesen werden.

Insgesamt wurden bei dieser Prüfung eine Vielzahl von Dateien wiederhergestellt: Von PDF- oder Excel-Dokumenten, über einzelne E-Mail-Dateien im EML-Format oder mehrere im MBOX-Format bis hin zu Fotos als Bitmap oder JPEG reichte die Ausbeute. Besonders problematisch war der Inhalt der Dateien: Neben einigen Bilddateien von Mitarbeitern hatte allein diese eine Platte äußerst sensible Informationen wie beispielsweise Signaturlisten, aktuelle E-Mail-Adressen oder Ansprechpartner im Unternehmen zu bieten. Richtig gefährlich war aber die auf der Festplatte vorhandene Geschäftskorrespondenz laufender Projekte. Für Datendiebe und Industriespione wäre diese Platte eine gute Informationsquelle, nicht nur um Diebstähle zu begehen, sondern auch Sabotage oder Erpressungen wären Tür und Tor geöffnet.

Da bei dieser Untersuchung herausgefunden werden sollte, ob sich trotz der geringen Sektorengröße überhaupt Daten rekonstruieren lassen, wurde keine defekte Festplatte getestet. Wenn es sich allerdings um eine ausgefallene Disk gehandelt hätte, wäre die Platte zunächst von den Spezialisten des Reinraumes physisch soweit wieder repariert worden, dass sie von einem Betriebssystem und speziellen Kroll Ontrack Software-Werkzeugen gelesen werden kann. Je nach Schwere des Defekts müssen dazu einzelne Teile der Festplatten entweder ausgetauscht oder repariert werden. Im nächsten Schritt würden dann die Inhalte der Platten wiederhergestellt.

An diesem Beispiel zeigt sich, dass gerade der Austausch von RAID-Festplatten aus einem aktiven Storage-System ein konkretes Risiko für den Datenschutz eines Unternehmens bedeutet.

Der Nachweis über die Wiederherstellbarkeit von Daten auch aus verhältnismäßig kleinen Stripe-Blöcken einer RAID-Festplatte beweist, dass bereits vor der Rückgabe einer RAID-Festplatte an den Hersteller Vorkehrungen getroffen werden müssen.

Sicher Löschen vor dem Austausch

Um eine ungewollte Wiederherstellung von Unternehmensdaten zu verhindern, bietet Kroll Ontrack verschiedene individuell angepasste Datenlösch-Services und -Produkte an: Neben der Möglichkeit eine der spezialisierten und zertifizierten Lösch-Software-Lösungen des finnischen Herstellers Blancco einzusetzen, lassen sich alle Daten einer RAID 6-Festplatte auch mit dem Ontrack Degausser sicher löschen. Durch das Degaussen (oder einer Entmagnetisierung) der Festplatte ist gewährleistet, dass die Festplatte weder ausgelesen noch jemals wieder eingesetzt werden kann. So wird ein hundertprozentiger Schutz vor Datenlecks beim Austausch von RAID-Festplatten gewährleistet.

Der Degausser kann durch seine kompakte Bauform praktisch an jedem beliebigen Ort innerhalb der IT-Abteilung aufgestellt werden und zerstört bei Bedarf innerhalb weniger Sekunden ausgefallene RAID-Festplatten, die für einen Austausch vorgesehen sind. Eine weitere sichere und finanziell tragfähige Lösung ist ein „Degaussen on Demand“, das Kroll Ontrack im Rahmen seiner Datenlöschungsservices anbietet. Dabei kommt ein Mitarbeiter zum Kunden vor Ort, löscht die RAID-Platte sicher und stellt über den Löschvorgang anschließend ein individuelles Zertifikat als Nachweis oder für Compliance-Zwecke aus. Mit diesen Angeboten und der Erweiterung seiner internen Datensicherungsstrategie um die Datenlöschung im Falle eines Festplatten-Austausch verhindern Unternehmen einfach und effektiv das Risiko eines ungewollten Datenlecks.

Kroll Ontrack