Zur Lage

WIK-Sicherheits Enquête® 2010/11

Bild: Arne Müseler (cc-sa 3.0)

Love-Parade 2010: Werden Lehren gezogen?

Unternehmensschutz

Bild: Alchemist-hp (CC BY-SA 3.0)

Head Crash – jetzt sind Profi-Datenretter gefordert.

Sicherheitstechnik

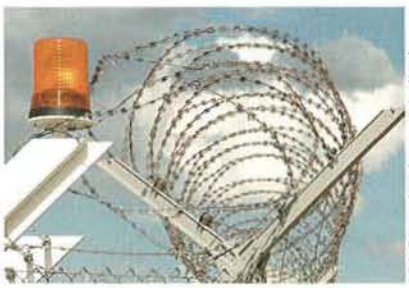


Bild: Dieter Poschmann/pixelio.de

Sicherheitsmarkt

Bild: Deutsche Messe AG

Mit neuem Konzept zu vollen Hallen?

Titelbild: VdS Schadenverhütung GmbH

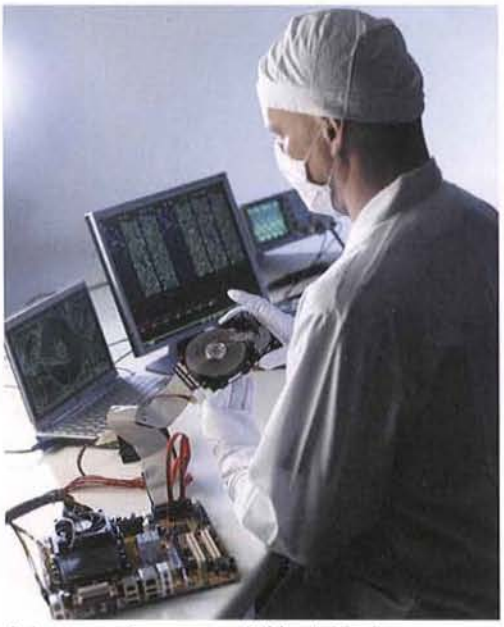
Datenrettung im Unternehmensschutz

So lässt sich ein Vabanque-Spiel mit sensiblen Daten vermeiden

Selbst Weltkonzerne kommen oft erst im Schadensfall auf die Idee, zur Rettung eines Datenträgers einen Spezialisten zu suchen. Allerdings ist die dann schon entstandene Panik ein schlechter Ratgeber: In der Hektik landet die Festplatte mit sensiblen Unternehmensdaten eventuell in unprofessionellen Händen oder gar im Ausland. Das kann fatale Konsequenzen haben, denn oft geht es nicht um versehentlich gelöschte Windows-Dateien – es geht um die Fälle, bei denen RAID-Systeme ganze Datenbestände beschädigt haben oder um Schäden durch Brand oder Überschwemmungen – mit der Frage, ob ein Unternehmen ohne diese Daten überhaupt weiterbestehen kann. Wie lassen sich die schlimmsten Fehler vermeiden?

Von Nicolas Ehrschwendner, Wien

Tatsächlich ist es so, dass ein Datenverlust oft zu Zeiten auftritt, an denen das Netzwerk nicht stark ausgelastet ist – also nachts oder an den Wochenenden. Der Grund dafür ist, dass zu diesen Zeiten Wartungsarbeiten erfolgen, Updates eingespielt oder Systemumstellungen durchgeführt werden. Kommt es dann zu Fehlfunktionen, ist der betreffende Mitarbeiter oft auf sich alleine gestellt, was eine massive psychische Belastung bedeutet – er steht unter dem enormen Druck, das System rasch wieder in Gang zu bringen. Tatsache ist aber auch, dass das Feld der Datenrettung komplex ist und oft genug selbst IT-Spezialisten überfordert, zumindest beim „ersten Mal". Ideal ist es, wenn sich Unternehmen bereits im Vorfeld beraten lassen, um auch hier korrekt zu reagieren.



Reinraum zur Datenrettung (Bilder: Attingo)

Auch erfolgt ein Anruf bei Datenrettungs-Unternehmen aus Unkenntnis der Sachlage in der Regel zu spät. Meist wird noch versucht, mit einfachen Methoden Daten wiederherzustellen. Doch oft wird genau durch diese Versuche der Schaden noch vergrößert, da etwa Daten gelöscht werden, die noch zu retten gewesen wären. Ein erster Ansprechpartner ist häufig auch der Lieferant des Systems, der „etwas probiert" oder auch der Hersteller. Bis der Datenträger dann endlich bei Spezialisten landet, haben schon viel zu viele Instanzen versucht, den Fehler zu beheben. Das vergrößert den Schaden enorm – zudem wird die Behebung teurer.

Sensible Unternehmensdaten in fremden Händen

Muss ein Datenträger außer Haus gegeben werden, spielen vor allem bei sensiblen Unternehmensdaten Sicherheitsüberlegungen bei der Auswahl des Datenretters sowie beim Ablauf eine große Rolle. So sollten Daten beim Datenrettungs-Unternehmen zum Beispiel nicht auf Servern abgelegt werden. Dort sollte nur mit physikalischen Kopien gearbeitet werden. Dadurch wird erreicht, dass physikalisch kein Zugang über das Netzwerk zu den Kundendaten möglich ist, denn Daten, die auf Servern abgelegt werden, stehen grundsätzlich unter dem Risiko, etwa im Zuge von Hacker-Attacken, ausspioniert zu werden. Manche Unternehmen legen Kundendaten routinemäßig auf einem Internet-Server ab, die dann von Technikern in anderen Ländern analysiert werden. Diese Übertragungen via Internet stellen definitiv ein Risiko dar.

Weitere Überlegungen:

- Unter welchen Voraussetzungen dürfen Daten außer Haus gegeben werden?
- Liegen gesetzliche Bestimmungen zur Weitergabe vor (Patientendaten, beschlagnahmte Datenträger von Gericht)?
- Sind auf den Daten Betriebsgeheimnisse enthalten (Konstruktionspläne), die für andere Unternehmen (auch ausländische) von Wert sein könnten?
- Wie stelle ich sicher, wo der Datenträger bearbeitet wird ? Ist die Adresse nur ein Office-Rental, ein Beratungs-Büro oder tatsächlich ein Labor?
- Werden Kopien vom Datenretter nach einer spezifizierten Zeit nach Abschluss des Falles gelöscht?

Wichtige Regeln im Falle eines Crashs

Diagnose

Datenretter bieten manchmal auch kostenlose Analysen an, allerdings sollte hier genau die Leistung unter die Lupe genommen werden. Nach Abschluss einer kostenpflichtigen Diagnose dagegen, sollte der Kunde einen Diagnosebericht erhalten, der den physikalischen und logischen Status des Datenträgers sowie das Volumen der Daten, die zu retten sind, beschreibt.

Angebot

Hier geht es vor allem um die Frage, ob ein Fixpreis angeboten wird. Die Gefahr bei Fixpreisen ist einerseits, dass der Preis im Verhältnis zum Aufwand zu hoch ist, und andererseits, dass ab einem bestimmten Punkt die Datenrettung nicht mehr durchgeführt wird, weil der Aufwand für den Datenretter den Fixpreis übersteigt. Als offizielle Begründung wird dann gerne angeführt, dass eine Wiederherstellung der Daten unmöglich sei – was in Wirklichkeit oft nicht richtig ist. Es empfiehlt sich, in einem solchen Fall vom Anbieter einen genauen Diagnosebericht zu verlangen, der beschreibt, warum eine Datenrettung nicht möglich war. Mit dieser Diagnose lässt sich dann ein weiterer Anbieter konsultieren.

Unseriös ist die Verrechnung nach Datenvolumen – der Aufwand der Datenrettung hängt nicht von der Anzahl der verlorenen Bits und Bytes ab, sondern ergibt sich vielmehr aus der Art des Fehlers und dem zugrunde liegenden System. Ein seriöser Anbieter verrechnet die Datenrettung immer nach Aufwand und gibt vorweg eine Preisspanne an, in der sich der Fall bewegen wird – somit kann sichergestellt werden, dass der Anbieter auch wirklich alles versucht, um die verlorenen Daten wieder zu bekommen. Ein renommierter Anbieter kann oft bereits aus der Fehlerbeschreibung eine solche Preisspanne angeben.

Tatsächlich zeigt erst die Untersuchung im Labor, wie teuer es wirklich wird. Ein verbindliches Angebot sollte dann erfolgen, wenn die Daten bereits gerettet sind. Der Kunde kann sich so dann noch immer entscheiden, ob er das Angebot annimmt oder nicht. Wenn eine Datenrettung nicht möglich ist, sollte das beauftragte Unternehmen die Kosten für den vergeblichen Aufwand tragen.

Verbranntes Notebook – die Daten sind trotzdem noch rekonstruierbar.

- Unterzeichnet der Datenretter eine Datenschutzvereinbarung?
- Wie wird der Datenträger vom Kunden ins Labor und retour transportiert? Ist ein persönliches Abgeben und Abholen im Labor möglich? Bietet der Datenretter einen Sicherheitstransport an? Bietet der Datenretter eine optionale verschlüsselte Auslieferung der rekonstruierten Daten an?

Auch sollte sich der Kunde darauf einstellen, dass rekonstruierte Daten stichprobenartig gesichtet werden – mit dem Zweck, zu überprüfen, ob die Rekonstruktion erfolgreich war. Es sei denn, dass eine Sichtung vertraglich ausgeschlossen wurde. Ein anderes Verhalten ist weder notwendig noch angebracht. Sollten dabei zufällig kriminelle Inhalte entdeckt werden, obliegt es dem Unternehmen Anzeige zu erstatten, ohne dazu verpflichtet zu sein. Anders liegt der Fall, wenn das Datenrettungs-Unternehmen direkt von zuständigen Behörden beauftragt wird, Daten einzusehen. Diese werden dann auch übermittelt.

Sonderfall verschlüsselte Festplatten

Festplatten, die aus Sicherheitsgründen verschlüsselt wurden, kommen sehr häufig vor. Große Unternehmen haben Sicherheitsrichtlinien, die eine automatische Verschlüsselung der Festplatten von Mitarbeiter-Laptops vorsehen. Dies ist für die Datenrettung kein Problem: Die Schlüssel sind dem Kunden ja in der Regel bekannt. Ist das Passwort nicht vorhanden, hängt es von der Qualität des Passworts und vom Verschlüsselungsalgorithmus ab, ob eine Rekonstruktion möglich ist. ▶

Fälle für die Datenrettung

Rachefeldzug

Eine große Handelsfirma hatte sich dazu entschlossen, einen mäßig erfolgreichen EDV-Betreuer zu wechseln. Der Mann nutzte den Umstand aus, dass seine Passwörter nicht sofort gesperrt wurden, loggte sich auf mehreren Servern des Unternehmens ein und löschte großflächig. Auf diese Weise legte er den kompletten Betrieb lahm. Die Daten konnten rekonstruiert werden.

Straftäter

Ein Kaufmann wollte eine Festplatte mit für ihn belastendem und verbotenem Pornomaterial vernichten. Er löschte die Daten und setzte die Platte unter Wasser und unter Strom, um einen Kurzschluss zu produzieren. Der Plan ging auf. Der Mann war jedoch gierig und gab die Platte, die noch Garantie hatte, zum Austausch an den Hersteller zurück. Als die Polizei den Mann aufgrund von Hinweisen später festnahm, konnte auch die Platte beim Hersteller noch sichergestellt und die belastenden pornografischen Bilddaten rekonstruieren werden.

Auf Abwegen

Wenn in der Pharmaforschung mehrere Terabyte an Studiendaten wegen eines defekten Servers verloren gehen, ist schnelle Hilfe angesagt. Doch drei beauftragte Unternehmen beschieden das Unternehmen, dass die Daten nicht mehr zu retten seien. Doch danach beauftragte und auf RAID-Systeme spezialisierten Techniker konnten mit einer speziellen Lösung helfen. Zusätzlich stellte sich heraus, dass der Server zuvor aus Kostengründen ohne Wissen des Kunden langwierig an Subdienstleister in Süd- und Osteuropa verschickt wurde, die jedoch versagt hatten.

Quelle: Attingo

Neugieriges Ausland?

Die Gefahr bei einer Datenrettung im Ausland ist primär in der Länge der Transportwege und der Qualität des Transportes zu sehen. Das Risiko eines solchen Transportes aus Profitinteressen, ohne Wissen des Kunden, ist als schwerer Vertrauensbruch zu werten. Ansonsten hängt die Qualität der Datenrettung eher von der Seriosität und dem Know-how des Technikers und der Ausstattung des Labors ab, nicht primär von dessen Standort. Dagegen reduzieren sich im Ausland die rechtlichen Möglichkeiten etwa im Fall von Schadensersatzansprüchen. Was passiert, wenn der Datenträger „nie ankommt" oder auf dem Rückweg verloren geht?

Allerdings sind keine Unternehmen bekannt, die lediglich dazu gegründet wurden, unter der Vorspiegelung Daten zu retten und an die kostbaren Inhalte zu kommen. Es ist aber als bekannt vorauszusetzen, dass in bestimmten Ländern Regierungsorganisationen über Mittel und Wege verfügen, auf private Unternehmen Einfluss zu nehmen.

Ob Ausland oder Heimatland, immer sollte auch schon die Webseite eines Anbieters, etwa das Impressum, auf Vollständigkeit und Plausibilität überprüft werden. Es gab Fälle, bei denen es sich durch diese Marginal-Überprüfung herausstellte, dass die Adresse des angeblichen Laborstandorts in Wahrheit der Sitz Dutzender Briefkastenfirmen war und die Festplatte dann doch ins Ausland geschickt wurde.

Auch Internetforen können – und hier sollte sich ein Verantwortlicher schon vor einem Schaden informieren – wichtige Anhaltspunkte sowie Beiträge und Erfahrungsberichte von betroffenen Personen bieten, die die Dienstleistungen eines Datenretters in Anspruch genommen haben. Fällt ein Unternehmen mehrfach negativ auf, ist dies ein erstes Alarmsignal. Und wer mit Privatanwendern schlecht umgeht, tut dies auch mit größeren Kunden.

Internetportale zur Erstinformation

- *www.wannago.de*
- *www.computerbase.de/forum/forumdisplay.php?f=78*
- *www.forum.chip.de/datensicherung-datenrettung*
- *www.tomshardware.de/foren/foren-10.html*

Über unseren Autor:

Nicolas Ehrschwendner begann ab 1992 mit dem Rekonstruieren von verlorenen Daten. Im Jahr 2004 beendete er das Studium Informatik auf der Technischen Universität Wien. Mittlerweile ist er Gesellschafter und Geschäftsführer von Attingo Datenrettung, die Niederlassungen mit eigenen Reinraumlabors in Wien, Hamburg und Amsterdam betreibt.
Kontakt: ne@attingo.com