IT Forensik - SOKO Datenrettung

Das Wiederherstellen von gelöschten Daten

Im Labor sitzen weiß gekleidete Personen mit Mundschutz und Sicherheitsbrille über einigen Festplatten. Man hört nur das gleichmäßige Atmen der Anwesenden und leise Geräusche der chirurgischen Instrumente. Auf dem Großbildschirm im Hintergrund laufen wirr Nullen und Einsen. Der leitende Forensiker spricht in sein Diktiergerät: „Festplatte, 1 GB, älteres Modell." Pause. „Firmenname nicht zu entziffern, Reste von der Seriennummer, meist unleserlich…" Pause. „Wir öffnen jetzt das Gehäuse. Vielleicht, wenn wir…" Der Rest ist unverständliches Gemurmel. Plötzlich hektisches Treiben im Labor bis der erlösende Ruf durch das Firmengebäude tönt: „Wir haben sie…!"

Leider geht es im Bereich der IT-Forensik nicht immer so spannend und geheimnisvoll zu, obwohl das schon ein imposanter Anblick wäre und dem Ego des einen oder anderen gut tun würde, doch ist Datenrettung weit von dem entfernt, was die CSI Forensiker im Fernsehen bieten. Meist ist Datenrettung ein viel nüchterneres Geschäft und nur in ganz gravierenden Fällen müssen Festplatten zur Datenrettung in ein Labor.
Die meisten Daten werden mit konventionellen Mitteln wieder hergestellt. Das Eigentliche und Wesentliche bei Datenverlusten ist es, Vorkehrungen zu treffen, dass es nicht (wieder) dazu kommt.

Erste Schritte

Doch beginnen wir chronologisch und der Wichtigkeit wegen mit dem Zeitpunkt x, an dem man feststellen muss, dass wichtige Daten gelöscht oder zerstört wurden. Um möglichst viele Daten zu retten, beziehungsweise wieder herzustellen, und die richtige Entscheidung zu treffen, wie und mit welche Aufwand die Daten rekonstruiert werden sollen, kann folgende Entscheidungsmatrix als Hilfestellung dienen:

1.) Daten identifizieren: Welche Daten sind betroffen?
2.) Bewertung der Daten: Was sind die gelöschten Daten für das Unternehmen wert? (Dabei sollten die Kosten der Wiederherstellung unter den Kosten der Neuerstellung durch den Benutzer liegen. Bei reinen Textdaten rechnet man ca. 1000 € / MB)
3.) Gibt es ein Backup der Daten oder könnten sie sonst noch irgendwo sein?

Worst Case stellt sich heraus, dass es sich um wichtige Daten handelt, die weder auf einem Backup zu finden sind, noch manuell, also durch erneute Eingabe, rekonstruiert werden können. In diesem Fall sollte das betroffene System umgehend vor weiteren Zugriffen geschützt werden, um seinen aktuellen Zustand zu sichern. Je weniger auf dem Datenspeicher geändert oder überschrieben wird, desto größer ist die Wahrscheinlichkeit die Daten wieder rekonstruieren zu können. Bei Client-Systemen kann das relativ einfach geschehen, indem es vom Netzwerk getrennt wird und der Benutzer das Arbeiten vorübergehend einstellt. Bei Netzwerk-Speichern muss das Gerät ebenfalls vor Zugriffen geschützt werden. Auch da ist das Trennen vom Netzwerk eigentlich unerlässlich, auch wenn einem Benutzer im Nacken sitzen. In diesem Fall ist die Bewertung der Daten besonders wichtig.

„Sicherung" des Systems

Der nächste Schritt ist, eine Kopie, ein Image vom betroffenen System zu erstellen, um die Datenwiederherstellung vorzubreiten. Im freien Markt gibt es viele Systeme, sowohl auf Software-, als auch auf Hardwarebasis, um ein Image zu erstellen. Meist reichen softwarebasierte Lösungen aus, denn man braucht kein gerichtsverwertbares Image. Hat man das Image erstellt, kann das Originalsystem wieder ans Netz gehen. Das Image sollte überprüft werden, bevor das Originalsystem wieder dem Produktiv-Betrieb zugeführt wird. Jetzt kann mit der Kopie des Images weitergearbeitet werden. Sollte man sich nicht trauen oder die Daten zu wichtig sein, so steht der Weg zu einem professionellen Datenrettungslabor natürlich jederzeit offen.

Die Wiederherstellung

Bei der Auswahl des Produktes zur Datenrettung sollte unbedingt darauf geachtet werden, dass es sich um kein Programm handelt, das zwingend in das betroffene System installiert werden will. Diese Programme vergrößern meistens den Schaden. Deshalb gilt: Nur mit dem Image arbeiten oder „Never touch the running system".
Normalerweise werden Daten auf einer Festplatte nicht gelöscht, sondern aus dem Inhaltsverzeichnis der Festplatte entfernt. Das Windows-System betrachtet diese Dateien als „gelöscht". Die entsprechende Software erkennt aber die Datenfragmente und setzt sie wieder zusammen. Ähnlich funktioniert es auch bei formatierten Festplatten, denn bei einer normalen Formatierung wird nur das „Inhaltsverzeichnis", der Index, gelöscht. Die Daten sind prinzipiell noch vorhanden.

Verfolgung einer Straftat

In den meisten Fällen kommt ein IT-Forensiker oder EDV-Sachverständiger dann zum Einsatz, wenn eine Straftat vorliegt. Sollte der Verdacht aufkommen, dass ein System manipuliert wurde, so ist es unerlässlich, das System sichern zu lassen. In diesem besonderen Fall spielt der Datenwert oder ein vorhandenes Backup eine untergeordnete Rolle. Das IT-System muss noch sorgfältiger behandelt werden, als ein Datenverlust von wertvollen Daten ohne Backup. Hier gilt besonders: System nicht verändern. Also das betroffene System vom Netzwerk trennen, auf keinen Fall herunterfahren (es könnten Skripts zur Löschung von Daten implementiert worden sein) und das Gerät physikalisch gegen fremde Zugriffe schützen. In jedem Fall sofort die Geschäftsleitung informieren und einen EDV-Sachverständigen einbeziehen. Je schneller und umfangreicher das System gesichert wird, desto eher lassen sich digitale Spuren des Verbrechens nachweisen. Auch in diesem Fall wird ein Image vom Originalsystem erstellt, um gelöschte Daten herzustellen und Verfahren zu rekonstruieren.
Ob in jedem Fall die Polizei eingeschaltet werden muss, liegt nicht allein in der Entscheidungsgewalt der Geschäftsführung. Es gibt Straftaten, die auf jeden Fall angezeigt werden müssen. Dazu gehören:

- Friedensverrat, Hochverrat, etc.
- Verunglimpfung des Staates und seiner Organe
- Straftaten gegen die öffentliche Ordnung (u.a Gewaltdarstellungen)
- Straftaten gegen die sexuelle Selbstbestimmung (insbesondere Kinderpornografie, deren bloßer Besitz bereits strafbar ist)
- Verletzung des persönlichen Lebens- und Geheimbereichs
- Diebstahl, Unterschlagung, Betrug und Untreue
- Vorbereitung einer Straftat

Eine Nichtanzeige der oben genannten Straftaten führt zur Mitwisserschaft, die ebenfalls strafrechtlich verfolgt werden kann. So ist man auf der sicheren Seite, derartige Delikte sofort zu melden, um eigener Strafverfolgung zu entgehen.

Datenwiederherstellung nach Katastrophen

Im Katastrophenfall, z.B. Brand, Hochwasser, Erdbeben oder andere physische Beschädigung der Datenträger, die sie in ihrer Funktionalität beeinträchtigen, bei Beschädigung der Datenträgerlogik, der Mechanik oder seiner Software, kann es nötig sein, die Dienste eines Forensik-Labors mit Reinraum hinzuzuziehen.
Da diese Dienste extrem kostspielig sind, sollte dabei auch nur auf die wichtigsten Datenträger zurückgegriffen werden. Sind die wiederherzustellenden Daten verschlüsselt, ist unbedingt der Server wieder herzustellen, der die Algorithmen der Verschlüsselung hält. Sind die Daten nicht verschlüsselt und die Rechtevergabe auf die Daten nicht allzu komplex, beziehungsweise nicht besonders durch Zugriffsrechte geschützt, kann in einigen Fällen auf die Wiederherstellung des Domänenkontrollers verzichtet werden.
In jedem Fall sind die Datenschutzrichtlinien einzuhalten.

... der Tag danach

Hat man nun das ganze Procedere der Datenwiederherstellung hinter sich, sollte man ernsthaft darüber nachdenken, dass solche Aktionen nicht noch einmal vorkommen. Eine regelmäßige und gut durchdachte Datensicherung ist in jedem Fall günstiger, als eine Datenwiederherstellung. Dabei sind die Möglichkeiten vielfältig. Angefangen beim konventionellen Backup mit Board-Mitteln, über Sicherungs-Software, bis hin zur Snap-Shot-Technik. In jedem Fall aber sollte regelmäßig eine (verschlüsselte) Kopie der Unternehmensdaten, inklusive der dazugehörigen Server (Verschlüsselung und Rechtevergabe) an einem externen Ort gelagert werden. Ein Schließfach in einer Bank oder ein Tresor in einer Filiale leisten dabei gute Dienste.