

Zusammenfassung

Man spricht von einem Datenverlust, wenn Daten gelöscht oder beschädigt werden, so dass kein Zugriff auf diese Daten mehr möglich ist. Diese Situation kann sich aufgrund verschiedenster natürlicher Ereignisse (Katastrophen), technischer Vorkommnisse (Störungen) oder aufgrund eines menschlichen Eingriffs (Diebstahl mit Zerstörung, beabsichtigte oder unbeabsichtigte Zerstörung) ergeben. Alle Benutzer von EDV-Ressourcen können von einem Datenverlust betroffen sein.

Angesichts der Vielzahl von Ereignissen, die zu einem Datenverlust führen können, müssen zahlreiche Schutzmaßnahmen berücksichtigt werden.

Ganz gleich, auf welche Ursachen er zurückzuführen ist - der Datenverlust ist leider ein in der Informatik häufig auftretendes Phänomen. Das vorliegende Dokument beschreibt die Risiken, die zu einem Datenverlust führen können. Außerdem enthält es vorbeugende Maßnahmen sowie Verfahren zur Datenwiederherstellung nach einer Katastrophe.

Inhalt

- 1 Was ist ein Datenverlust? →
- 2 Wer ist betroffen? →
- 3 Was sind die Hauptbedrohungen? →
- 4 Statistiken →
- 5 Vorbeugende Maßnahmen →



1 Was ist ein Datenverlust?

Man spricht von einem Datenverlust, wenn Daten gelöscht oder beschädigt werden, so dass kein Zugriff auf diese Daten mehr möglich ist. Diese Situation kann sich aufgrund verschiedenster natürlicher Ereignisse (Katastrophen), technischer Vorkommnisse (Störungen) oder aufgrund eines menschlichen Eingriffs (Diebstahl mit Zerstörung, beabsichtigte oder unbeabsichtigte Zerstörung) ergeben.

Dagegen spricht man von einer Datenänderung, wenn ein Teil der Daten verändert wurde, ohne dass jedoch dadurch kein Zugriff auf die Daten mehr möglich ist.

Als Datendiebstahl wird der Vorgang bezeichnet, wenn eine Person auf Daten zugreift, zu denen sie normalerweise keinen Zugang besitzt, und sich dieser Daten dann bemächtigt. Der Datendiebstahl kann per Kopie, Datenübertragung oder Ausdruck der Daten erfolgen. Der Datendiebstahl kann in Kombination mit einer anschließenden Vernichtung oder Veränderung der Daten erfolgen.

Um dieses Phänomen und die Mittel zur Wiederherstellung besser verstehen zu können, müssen folgende Unterscheidungen beachtet werden:

1.1 Datenverlust aufgrund eines nicht mehr möglichen Zugriffs auf die Daten

Diverses raisons physiques ou logiques peuvent provoquer la perte d'accès aux données. Dans la majorité des cas, les données sont encore physiquement stockées sur les supports informatiques, mais puisqu'ils ne sont plus accessibles, on parle de perte de données. Les méthodes de récupérations se distinguent des méthodes utilisées pour récupérer des données détériorées ou supprimées.

1.2 Datenverlust aufgrund einer Veränderung der Daten

Bestimmte von Piraten an Web-Servern durchgeführte bösartige Manipulations führen nicht zur Vernichtung oder zum Diebstahl der Daten, sondern lediglich zu deren Veränderung. So kann ein "Hacker" beispielsweise bekannt gegen, an irgend einer Stelle einfach nur einen einzigen Datensatz verändert zu haben. In diesem Fall kann auf die ursprünglichen Daten nicht mehr zugegriffen werden, da sie verändert wurden, was ebenfalls einem Datenverlust entspricht.

Der Datenverlust aufgrund einer Veränderung der Daten kann auch durch absichtlich oder unabsichtlich an Datenbanken oder Dateien vorgenommene unerlaubte Aktionen erfolgen.

Der Datenverlust aufgrund einer Veränderung der Daten kann auch durch absichtlich oder unabsichtlich an Datenbanken oder Dateien vorgenommene unerlaubte Aktionen erfolgen.

1.3 Datenverlust durch Datendiebstahl

Ein Datendiebstahl führt nicht unbedingt zur Vernichtung, Beschädigung oder zur Veränderung der Daten. Wenn die Daten kopiert, übertragen oder ausgedruckt werden, bleiben die ursprünglichen Daten unverändert. Dies ist übrigens einer der Gründe, warum sich ein Datendiebstahl manchmal nur schwer feststellen lässt.

Die Auswirkungen eines Diebstahls vertraulicher Daten (zum Beispiel Fabrikationsgeheimnisse) können deutlich höher sein als die bei einem einfachen Datenverlust. Man spricht auch von einem Verlust des Datengeheimnisses.

1.4 Datenverlust durch Diebstahl oder Geräte- bzw. Datenträgerverlust

Der Verlust oder Diebstahl von portablen Computern und von jeglicher Art von Datenträgern (Magnetband, Diskette, CD ROM (Compact Disk Read Only Memory) etc.) ist häufig mit einem Verlust der auf diesen EDV-Ressourcen gespeicherten Daten verbunden. Die Benutzer dieser Datenträger verfügen nur in seltenen Fällen über eine vollständige Sicherungskopie. Der Diebstahl oder Verlust von Datenträgern stellt außerdem hinsichtlich des Verlusts des Datengeheimnisses ein hohes Risiko dar.

1.5 Datenverlust durch beabsichtigte Zerstörung bzw. Vernichtung der Daten

Wenn der Verlust oder die Veränderung der Daten nicht auf ein technisches Phänomen sondern vielmehr auf einen menschlichen Eingriff zurückzuführen ist, muss zwischen den folgenden Aktionen unterschieden werden:

- ➔ absichtliches, bösartiges Vorgehen (Zerstörung einer Web-Seite)
- ➔ absichtliches, nicht bösartiges Vorgehen (Löschen einer Datei)
- ➔ flchedte unabsichtliches Vorgehen (Bedienungsfehler).

3 Was sind die Hauptbedrohungen?

Laut der von den großen und auf die Wiederherstellung von Daten spezialisierten Unternehmen erstellten Statistiken geben die Benutzer als Hauptgründe für einen Datenverlust Folgendes an:

- ➔ 44 % Ausfälle der Hardware oder des Betriebssystems,
- ➔ 32 % menschliche Fehler,
- ➔ 14 % Beschädigungen der Software oder absichtliche Veränderungen der Software,
- ➔ 07 % Viren,
- ➔ 03 % Naturkatastrophen.

2

Wer ist betroffen?

Jeder Benutzer einer EDV-Ressource kann potenziell mit einem Datenverlust konfrontiert werden. Niemand ist davor gefeit. Es können jedoch verschiedene Maßnahmen ergriffen werden, um die Risiken zu minimieren oder diese Daten ganz oder wenigstens teilweise wiederherzustellen.

Ein Datenverlust kann sich aufgrund von Problemen im Zusammenhang mit der Funktionsweise oder Bedienung folgender Datenträger ergeben:

- ➔ Großrechner, mit denen Rechenzentren ausgestattet sind
- ➔ Server
- ➔ PCs
- ➔ Portable Computer
- ➔ Magnetische oder optische Datenträger.

Häufig sind die Opfer eines Datenverlusts nur zufällig betroffen. Viele "Hacker" beispielsweise wählen Ihr Ziel nur zufällig aus. Gleiches gilt natürlich für natürliche Ereignisse. Auch der Typ der verlorenen Daten kann ganz unterschiedlich sein:

- ➔ Öffentlich erhältliche oder intern entwickelte Softwareprogramme,
- ➔ Daten von geringerem Wert (Korrespondenz etc.),
- ➔ Kritische Daten, die für einen ordnungsgemäßen Betrieb des Unternehmens erforderlich sind (Daten des Rechnungswesens etc.),
- ➔ Strategische Daten (beispielsweise Fabrikationsgeheimnisse).

Diese Statistiken müssen mit Vorsicht betrachtet werden, da sie nur die Unternehmen umfassen, die einen Datenverlust beklagt und daraufhin ein Unternehmen mit der Wiederherstellung beauftragt haben. Das bedeutet, dass diese Statistik nur in ganz begrenztem Umfang den Verlust von nicht kritischen Daten einschließt, da in einem solchen Fall selten ein die Dienste eines speziellen Unternehmens in Anspruch genommen werden. Außerdem umfasst diese Statistik keine Unternehmen/Verwaltungen/Privatpersonen, die die Daten mit eigenen Mitteln wiederherstellen konnten oder die ihre möglichen Datenverluste nicht öffentlich bekannt geben wollten, um ihr Markenimage aufrecht zu erhalten.

4

Statistiken

Die in diesem Abschnitt aufgeführten Statistiken geben einen Überblick über das Ausmaß der Problematik.

4.1 Portable Computer

50% der Geschäftsreisenden verfügen über keinen Schutz gegen den Datenverlust, obwohl 80% ihrer Informationen auf ihrem portablen Computer gespeichert sind (Quelle: IDC - International Data Corporation).

4.2 Die betroffenen Bereiche

Zu diesem Thema hat der CLUSIF (Club de la Sécurité des Systèmes d'Information Français) im Jahr 2002 einen Bericht veröffentlicht, der alle Wirtschaftsbereiche umfasst und die Schadenhäufigkeit im EDV-Bereich angibt.

Er enthält interessante Informationen hinsichtlich der betroffenen Bereiche und hebt weniger bekannte Aspekte wie beispielsweise die Verantwortung von Unternehmen gegenüber Dritten und Vermögensverluste hervor (der Bericht umfasst jedoch nicht Analysen bezüglich Verwaltungen oder Privatpersonen).

- ➔ Kosten für die Reparatur oder den Ersatz von beschädigter oder fehlender Hardware: 21%.
- ➔ Kosten für die Wiederherstellung von beschädigten oder verloren gegangenen Daten, Softwareprogrammen oder Verfahren: 18%.
- ➔ Verlust der Betriebsfähigkeit: 17%.
- ➔ Kosten für die Verstärkung der Schutzmaßnahmen: 16%.
- ➔ Haftung durch das Unternehmen: 15%.
- ➔ Vermögensverluste: 14%.

Aufteilung der sich aus Datenverlusten ergebenden finanziellen Auswirkungen (Quelle: CLUSIF)

HINWEIS

Es sei darauf hingewiesen, dass der mögliche Verlust der Betriebsfähigkeit natürlich viel höher als die Kosten für einen Ersatz der Geräte ist. Die offensichtliche Homogenität zwischen den verschiedenen, durch einen Datenverlust bedingten Auswirkungen ist auf die Tatsache zurückzuführen, dass alle Vorfälle nicht unbedingt zum Verlust der Betriebsfähigkeit führen.

5

Vorbeugende Maßnahmen

Dieses Kapitel beschreibt nur kurz die verschiedenen Gegenmaßnahmen, da einige dieser Maßnahmen in einem separaten Dokument beschrieben sind, um alle erforderlichen Erläuterungen aufzuführen.

Zunächst einmal muss zwischen den vorbeugenden Maßnahmen und den Maßnahmen zur Wiederherstellung nach einem Datenverlust unterschieden werden.

Es versteht sich von selbst, dass sich dieses Kapitel selektiv und abhängig vom Ausmaß und der Komplexität des betroffenen EDV-Geräts mit dem Thema beschäftigt.

5.1 Vorbeugende Maßnahmen

Unter diesem Punkt sind alle Maßnahmen zusammengefasst, die mit dem Ziel ergriffen werden, das Eintreten eines Ereignisses zu verhindern, das zu einem Datenverlust führen kann. Es sind aber auch die Maßnahmen aufgeführt, die eine Begrenzung der Schäden zum Ziel haben.

5.1.1. ANPASSUNG DER SPEICHERUNGSLÖSUNG

Die Datenspeicherverfahren sind an den Grad der Sensibilität der Daten sowie an den Datentyp (Dateien der Bürokommunikation, Datenbanken) anzupassen

Um eine schnelle Verstopfung der Speicherinfrastruktur und alle damit verbundenen Probleme zu vermeiden, ist es erforderlich, ein Dateiarchivierungsverfahren auf geeigneten Datenträgern einzufügen

Es empfiehlt sich, Server mit der RAID-Technologie (Redundant Array of Independent/Inexpensive Disks) auszustatten, die es ermöglicht, die Datenspeicherung auf mehrere Festplatten aufzuteilen. Bei einem Ausfall oder Verlust einer der Festplatten des RAID-Systems ist das EDV-System in der Lage, die fehlenden Daten wiederherzustellen. Es gibt verschiedene RAID-Konfigurationsebenen, die in einem separaten Dokument beschrieben sind.

Für große Infrastrukturen oder die Einrichtung einer zweiten Produktionsstätte kann sich auch die Implementierung eines Speichernetzwerks (SAN=Storage Area Network) als nützlich erweisen. Dieser Systemtyp erfordert spezielle EDV-Kenntnisse, und es wird geraten, sich bei Bedarf an ein spezielles Unternehmen zu wenden.

5.1.2. GEEIGNETE SPEICHERUNGS- /WIEDERHERSTELLUNGSVERFAHREN

Die Datenwiederherstellungstechnologien und -verfahren sind an den Grad der Sensibilität der Daten aber auch an den Datentyp (Dateien der Bürokommunikation, Datenbanken) anzupassen.

Technologien wie das "Snapshooting", dessen Ziel die Erstellung eines Abbilds der Datenbank während des laufenden Betriebs ist, verhindern im Fall eines Datenverlusts, zum Stand vom Vortag zurückkehren zu müssen. Auf diese Weise wird die erneute Eingabe der Daten oder die möglicherweise erforderliche erneute Verschlüsselung vermieden. Diese kostspielige und aufwendige Technik ist ideal für einen sehr komplexen Nutzungstyp, ist jedoch für die Sicherung der üblichen Bürodaten nicht von Interesse.

Die Einführung von allen Anwendern bekannten Verfahren, die eingehalten und überwacht werden, ermöglicht eine bestmögliche Nutzung der vorhandenen Infrastruktur. Als Beispiel für ein derartiges Verfahren kann die den Benutzern mitgeteilte Information bezüglich der täglich zu sichernden Verzeichnisse angeführt werden.

Die für die Wiederherstellung der Daten erforderliche Zeit ist leider ein häufig unterschätztes Kriterium. Die meisten EDV-Verantwortlichen sorgen sich in der Tat hauptsächlich um die Geschwindigkeit der Sicherung, ignorieren jedoch die Dauer einer möglichen Wiederherstellung. Bei einem Datenverlust ist jedoch die Wiederherstellung von entscheidender Bedeutung. Eine ausführliche Analyse der Wiederherstellungsarchitektur sowie des Netzwerks, bestätigt durch einen Test, stellt das beste Mittel dar, um festzustellen, ob die Lösung den Anforderungen entspricht.

5.1.3. EINHALTUNG VON MUSTERVERFAHREN IM BEREICH DER RECHENZENTREN

Die Implementierung einer EDV-Architektur muss bestimmten Anforderungen an die Umgebungsbedingungen entsprechen. Ein Rechenzentrum, eine Verbindungszentrale, ein Telekommunikationszentrum etc. müssen so ausgestattet sein, dass optimale Betriebsbedingungen für die Geräte gewährleistet sind. Dies umfasst: eine Notstromversorgung oder ein UPS (Uninterruptible Power Supply), eine Klimatisierung und eine Luftfilterung, eine Überwachung der statischen Elektrizität, ein spezielles System zur Bekämpfung von Wasser- und Brandschäden und eine Zugangskontrolle.

All diese Punkte sind in einem Dokument bezüglich der physikalischen Sicherheit beschrieben.

5.1.4. STOCKAGE ADAPTÉ DES SUPPORTS

Les supports informatiques, tels que les bandes magnétiques, supports optiques et autres doivent absolument être stockés dans des endroits répondant à leurs exigences en matière de protection contre la poussière, les griffes, l'humidité et autres facteurs pouvant les dégrader.

Es wird geraten, die Datenträger mit den Sicherungskopien in einem Tresor außerhalb des Rechenzentrums bzw. in einem anderen Gebäude aufzubewahren.

5.1.5. VERWALTUNG DER BENUTZERRECHTE

Die sicherste Möglichkeit, das unbeabsichtigte Löschen von Daten zu vermeiden, ist die Einschränkung der Benutzerrechte für den Zugriff auf die kritischen Dateien und Datenträger.

5.1.6. AKTIVE VERWALTUNG DES GESAMTEN EDV-SYSTEMS

Die meisten Funktionsstörungen, von denen die EDV-Geräte betroffen sind, kündigen sich zuvor an. Die meisten Geräte werden mit einem Softwareprogramm geliefert, das diese Vorboten erkennt und den Benutzer im Zweifelsfall warnt. Diese Softwareprogramme existieren sowohl auf Server- als auch auf PC-Ebene (Workstations) und sogar für portable Computer. Es wird geraten, diese Software ihre Arbeit machen zu lassen und die eventuell von ihr gelieferten Warnungen zu berücksichtigen.

5.1.7. SCHULUNG DER BENUTZER

Ein wichtiges Mittel zur Vermeidung von Fehlfunktionen ist die Schulung der Benutzer bezüglich der richtigen Bedienung des Geräts und der Peripheriegeräte sowie der Verwaltung der Daten und Verzeichnisse.

5.2 Maßnahmen zur Wiederherstellung

Unter diesem Punkt sind alle Maßnahmen zur Wiederherstellung der Daten nach einem Datenverlust aufgeführt.

5.2.1. AUF DIE WIEDERHERSTELLUNG SPEZIALISIERTE SOFTWAREPROGRAMME ODER UNTERNEHMEN

Es gibt zahlreiche Softwareprogramme, die in der Lage sind, die auf den unterschiedlichsten Datenträgern verloren gegangenen oder gelöschten Daten wiederherzustellen. Diese Softwareprogramme sind relativ teuer, und ihre Anwendung erfordert einige Kenntnisse auf diesem Gebiet. Es wird daher dringend geraten, sich bei Bedarf an ein auf diesem Gebiet spezialisiertes Unternehmen zu wenden.

5.2.2. WAS IST "FORENSIC" ?

"Forensic" ist ein englischer Begriff, der "gerichtliche Untersuchung" bedeutet. Diese Technologie besteht in der Suche nach Ereignissen, die zu einem Schadensfall geführt haben könnten.

Diese Technologie hat also zum Ziel, normalerweise nicht offenkundige Informationen über die Tatsachen zu erhalten, die zum Schadensfall geführt haben. Auf diese Weise soll der tatsächliche Grund des Datenverlusts herausgefunden sowie der Verursacher ermittelt werden. Diese Technologie hat also nicht direkt die Wiederherstellung von Daten sondern die Ermittlung der Ursachen, die zum Verlust geführt haben, zum Ziel.

Allein dieses Verfahren ermöglicht es, ein Verfahren gegen einen möglichen Piraten einzuleiten. Angesichts der Komplexität der Nutzung dieser Hilfsmittel und um den legalen Charakter dieser Beweise aufrecht zu erhalten, wird jedoch empfohlen, ein auf diesem Gebiet spezialisiertes Unternehmen zu beauftragen.

→ HINWEIS :

Sicherheitsbewusste Personen werden auf die Tatsache hingewiesen, dass man gelöschte Dateien wiederherstellen kann. Es ist jedoch jederzeit möglich, diese Art der Wiederherstellung zu deaktivieren. Auf diesen Punkt sollte besonders bei einem Wiederverkauf von EDV-Geräten geachtet werden.