Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

Proseminar – Speicher- und Dateisysteme

Datenwiederherstellung

Nicolas Petereit, 25.02.2018

Inhaltsverzeichnis

1. Einleitung

In den letzten Jahren ist die Menge an Daten durch die Entwicklungen in der Informatik exponentiell gestiegen. Da heute ganze Wirtschaftszweige und ein Großteil der Gesellschaft von Daten abhängt, muss ein verstärktes Augenmerk auf deren Sicherheit gelegt werden.

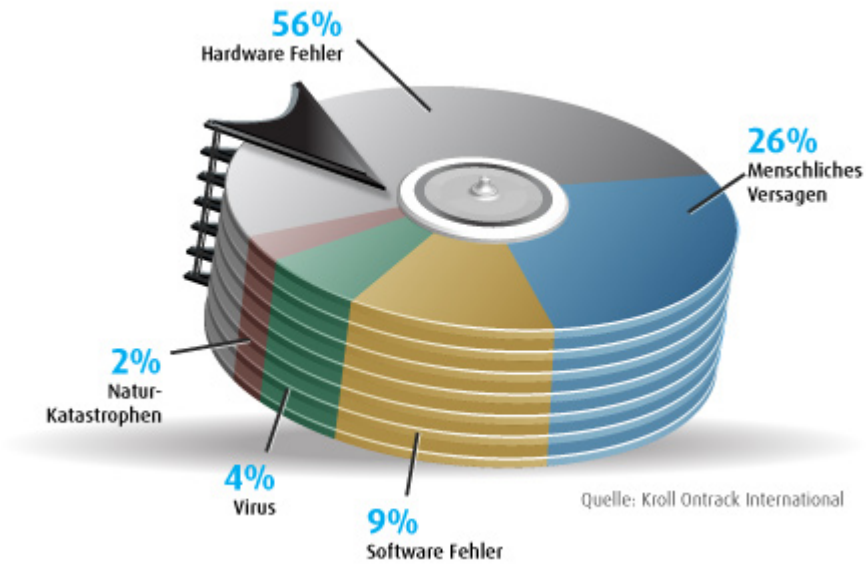
Ein wichtiger Bestandteil von Datensicherheit ist deren Verfügbarkeit, welche gerade durch Datenverlust eingeschränkt wird.

Aus diesem Grund werde ich im Folgenden einen Überblick geben, wie man Datenverlust anhand von Präventions- und Wiederherstellungsmaßnahmen verhindern kann.

2. Datenwiederherstellung

2.1 Verlustarten

Um die verschiedenen Ansätze zur Datenwiederherstellung zu verstehen, sollten vorher die typischen Verlustarten von Daten kurz betrachtet werden.



Wie an obiger Grafik zu erkennen ist, machen Hardwarefehler den größten Anteil an Datenverlusten aus.

Dabei lassen sich zwischen *Predictable Failures* und *Unpredictable Failures* unterscheiden.

Erstere zeichnen sich besonders durch ihre (theoretische) Vorhersehbarkeit aus. Es handelt sich dabei meist um einen Hardwareausfall der durch Abnutzung entsteht. Für die meisten typischen Hardwareteile ist eine durchschnittliche Lebensdauer bei sachgemäßer Nutzung bekannt, wodurch die Vorhersehbarkeit eines Ausfalls entsteht.

Im Gegensatz dazu kann es durch unsachgemäßen Umgang zu *Unpredictable Failures* führen, da dieser die erwartete Lebensdauer deutlich verringern kann. Dazu zählt zum Beispiel falsches Lagern, Herunterfahren oder Entfernen von Komponenten. Aber auch Naturkatastrophen wie Wasserschäden oder Brände können dazu gezählt werden.

Als zweitgrößter Verlustgrund gilt das *Menschliche Versagen*. Während Fehler wie das fälschliche Löschen oder Überschreiben von Daten das offensichtlichste Problem darstellen, können auch viele andere Ursachen indirekt auf menschliches Versagen zurückgeführt werden.

So können zum Beispiel unzureichende Sicherheitsmaßnahmen zu Viren oder sonstiger Manipulation von außen führen, oder oben genannter unsachgemäßer Umgang zu Hardwaredefekten.

Auch Softwarefehler können zu Datenverlust führen. Dies kann unter anderem durch Datenkorruption bei System/Programmabstürzen geschehen, aber auch in manchen Fällen durch fehlende Rückwärtskompatibilität (Beispiel: Ältere Daten können nach einem Softwareupgrade nicht mehr gelesen werden).

2.2 Datensicherung

Um die Sicherheit von Daten zu gewährleisten, sind entsprechende Präventionsmaßnahmen unumgänglich. Diese sollten durch ein Datensicherungkonzept deklariert und umgesetzt werden.

Dabei wird festgelegt, welche Daten wie oft und auf welche Weise gesichert werden sollen. Um im Notfall vorbereitet zu sein, sollten natürlich regelmäßig Wiederherstellungstests durchgeführt werden.
Folgende Tabelle gibt einen kurzen Überblick über mögliche Sicherungsmethoden, um schon den Verlust von Daten möglichst gering zu halten.

Art	**Beispiele**	**Hilft bei**
Erschwerung von Löschen/ Manipulation	-Verschlüsselung von Daten -Zugriff auf wichtige Daten einschränken	-Menschlichen Fehlern -Manipulation von außen
Hardware-Instand-haltung	-regelmäßiger Austausch von Hardware -geeignete Umweltbedingungen bereitstellen (Temperatur, Feuchtigkeit...)	-Hardwaredefekt/ *Predictable Failures*
Katastrophen-plan	-Notstromversorgung -Brandschutzmaßnahmen	-(Natur)katastrophen/ *Unpredictable Failures*

Art	Beispiele	Hilft bei
Backup	-vollständiges, regelmäßiges Kopieren der Speichermedien und deren separate Lagerung -mehrfaches Abspeichern wichtiger Daten	-allen genannten Verlustarten, da es egal ist wie die Daten verloren gegangen sind, wenn es eine Kopie davon gibt
RAID	-doppeltes Abspeichern aller Daten auf 2. Festplatte (*Mirroring*)	-Hardwaredefekt

2.3 Datenrettung

Wenn der Fall eintritt, dass doch einmal wichtige Daten verloren gehen, gibt es verschiedene Vorgehensweisen, bei denen versucht wird, soviele Daten wie möglich zu retten.

Eine davon ist das Auslesen des *unallocated space*, welche ich im Folgenden etwas genauer beschreiben werde.

Zuerst muss geklärt werden, wie Daten in einem klassischen Dateisystem wie NTFS gelöscht werden.

In jedem Dateisystem gibt es eine Art Inhaltsverzeichnis (in unserem Fall die *Master-File-Table*), in dem der Speicherort aller Daten eingetragen ist. Bei einem normalen Löschvorgang wird nun in diesem Inhaltsverzeichnis die Datei als gelöscht markiert; für das System wird dieser Speicherort nun für neue Daten freigegeben.

Solange dieser *nicht zugeordnete Speicherplatz* (Eng.*: unallocated space*) nicht von einer neuen Datei überschrieben wird, bleibt die ursprüngliche Datei jedoch vorhanden.

Diese Tatsache kann man sich bei der Datenrettung zu Nutze machen.

Wenn also eine Datenverlust festgestellt wird, sollte als erstes sofort das Speichermedium getrennt/abgeschaltet werden. Eine weitere Verwendung erhöht sonst das Risiko, dass der *unallocated space* von neuen Daten überschrieben wird.

Sollte es sich um einen Hardwaredefekt handeln, müssen eventuell vorher einige Komponenten repariert oder ausgewechselt werden. Dies sollte jedoch nur von Experten ausgeführt werden, da dabei die Gefahr einer totalen Beschädigung des Datenträgers herrscht.

Weiterhin ist es ratsam, zuerst eine Masterkopie von dem Datenträger zu erstellen und dann jeweils verschiedene Arbeitskopien davon zu machen. Dies ist wichtig, da besonders bei beschädigten Speichermedien nicht garantiert werden kann, dass das Original lange verwendbar ist. Die Arbeitskopien sind notwendig, damit immer eine unveränderte Kopie des Originals bestehen bleibt.

Nun können durch verschiedene Methoden und Tools viele Dateien gefunden und wiederhergestellt werden, bei dem unter anderem der *unallocated space* durchsucht wird.

Selbst für Laien gibt es viele effektive Programme, die sich gerade bei unwichtigeren Daten lohnen, bei denen ein Experte zu teuer wäre.

3. Sicheres Löschen

Bisher haben wir uns nur mit der Wiederherstellung von Daten beschäftigt, bei denen der Besitzer dieser Daten mit einer Wiederherstellung einverstanden ist.

In der Realität gibt es aber auch viele Situationen, in denen dies nicht der Fall ist.

So gibt es zum Beispiel das Fachgebiet der *IT-Forensik*, was sich damit beschäftigt, Kriminalfälle anhand von *digitaler Spurensicherung* zu lösen. Dabei werden Methoden der Datenwiederherstellung angewendet, um Daten zu erhalten, die eventuell gar nicht gefunden werden sollen. Häufig wurden dabei vorher Techniken verwendet, die das Wiederherstellen noch erschweren sollen.

Da eine Datenwiederherstellung aber genau so gut von potenziellen Angreifern benutzt werden können, ist es besonders bei der Handhabung von sensiblen Daten wichtig, sich auch mit der anderen Seite der Medaille zu beschäftigen.

Gerade bei der Entsorgung von benutzten Datenträgern ist dabei zu beachten, dass Daten nicht wiederhergestellt werden können. Dies kann zum Beispiel durch Zerstörung des Speichermediums, Verschlüsselung der Daten oder *Sicheres Löschen* geschehen. Beim *Sicheren Löschen* werden die Daten nicht nur gelöscht, sondern auch mit neuen Daten überschrieben. Dies verhindert häufig unter anderem den unter Abschnitt 2.3 genannten Rettungsansatz.

4. Fazit

Bei allen vorgestellten Sicherungs-, Wiederherstellungs-, und Löschmethoden gilt: Je mehr Methoden verwendet werden desto besser das Ergebnis. Jedoch ist dabei überall auf die Wirtschaftlichkeit zu achten. Bei der sogenannten Kosten-Nutzen-Analyse werden die Kosten der Methode mit dem Nutzen des Ergebnisses bzw. dem Wert der Daten verglichen.

Wenn einem die eigenen Daten wichtig sind, gibt es also einige Grundsätze, an die man sich halten sollte:

Im Idealfall sollte man nur im Notfall auf eine Datenwiederherstellung zurückgreifen müssen. Gibt es eine ausreichende Datensicherung, kann eine Wiederherstellung theoretisch überflüssig gemacht werden.

Es ist davon auszugehen, dass alle Daten irgendwann verloren gehen können. Wichtig ist also, gut darauf vorbereitet zu sein.

Falls doch einmal Daten verloren gehen, ist es wichtig, schnell zu handeln und im Notfall lieber Experten zu fragen.

Gerade bei häufigen Datensicherungen und Backups muss darauf geachtet werden, dass sensible Daten unzugänglich und unwiederherstellbar für Unbefugte bleiben.

5. Quellenverzeichnis

https://assets.krollontrack.com/hv3/images/img_ursachen-datenverlust_krollontrack.jpg

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html

https://www.cubespotter.de/cubespotter/it-forensik-digitale-spurensuche/

http://www.admin-magazin.de/Das-Heft/2013/11/Forensische-Toolkits-zur-Rekonstruktion-von-Browser-Sessions

https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html

https://www.pcwelt.de/ratgeber/Was-genau-passiert-beim-Loeschen-von-Daten-Ratgeber-Datenrettung-182351.html

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/Datenverlust/datenverlust_node.html

http://www.pc-magazin.de/ratgeber/ssd-flash-geloeschte-daten-wiederherstellen-datenrettung-tools-download-tipps-2111154.html

https://www.brandmauer.de/blog/it-security/was-sind-die-wesentlichen-ursachen-fuer-datenverlust

https://public.dhe.ibm.com/common/ssi/ecm/wr/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reportswrl12345usen-20170719.pdf

https://svs.informatik.uni-hamburg.de/teaching/gss-10einfsi.pdf

Datenwiederherstellung – 5. Quellenverzeichnis

wikipedia.org

https://de.slideshare.net/TobiasScheible/vortrag-zum-thema-digitale-forensik

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-de-4/s1-response-plan.html

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

https://svs.informatik.uni-hamburg.de/teaching/gss-20resi.pdf

https://www.storagecraft.com/blog/5-reasons-raid-not-backup/

https://www.youtube.com/watch?v=bYHsClMdJUs

http://datasecurityinc.com/security/degausser.html

https://www.intersoft-consulting.de/it-forensik/it-forensik-praxisfaelle/

https://www.storagecraft.com/blog/5-reasons-raid-not-backup/

http://www.searchsecurity.de/definition/Security-Information-and-Event-Management-SIEM

https://public.dhe.ibm.com/common/ssi/ecm/wr/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reportswrl12345usen-20170719.pdf

www.krollontrack.de