Festplatten wurden gelöscht

Beitrag von „BigHackintosh“ vom 11. Januar 2021, 14:11

> Zitat von Sascha_77
>
> Aber wenn er wirklich 1:1 diesen Befehl hier verwendet hat, fällt die Theorie doch eher raus:

Nun, ich weiß nicht was er kopiert hat, aber Daten löschen sich nicht einfach so. Zumal ich niemals einen rekursiven Löschbefehl einfach mittels C&P in die Shell kloppen würde. Entweder tippe ich den Befehl nach und kloppe ständig auf die Tab-Taste, damit er mir die Pfade (insbesondere diejenigen mit Leerzeichen) ergänzt oder aber ich setze das Ganze in Quotes. Ich hatte mich oben auch verschrieben und meinte natürlich hinter dem Slash und nicht davor... Wahrscheinlich ist es, dass er einen Backslash zum maskieren des Leerzeichens mit einem Slash verwechselt hat und dann ist auf jeden Fall die Wurzel weg, da "rm" mehrere Argumente akzeptiert. Ganz egal wie es passiert ist - die Daten sind erstmal weg und grundsätzlich - wenn die Platte nicht sofort ausgehangen wurde - bereits mit anderen Dingen überschrieben.

> Zitat von maexxx
>
> Hab jetzt unter macOS Disk Drill drüber laufen lassen, knapp 18 Std und er hat nur ca. 1 TB an Daten gefunden obwohl es um die 6 TB waren.

Das Programm muss bis zum Ende durchlaufen, da dies ein Journal-Filesystem ist und die Blöcke wahllos auf die Platte geschrieben werden. Meist gerade wo der Lese/Schreibkopf steht und freier Speicherplatz vorhanden ist. Es kann sein, dass die Daten ganz am Ende der Platte stehen. Da es sich hierbei um ein Journal-Filesystem handelt, wird halt nicht nur der Bezug zur Datei gelöscht, sondern auch der Bezug zu den einzelnen Blöcken.

Wenn du auf der Platte mehrfach herumgehampelt bist (deswegen schrieb ich, dass die Platte auf keinen Fall mehr schreibend gemountet werden soll und dies passiert, wenn man MacOS zig mal hoch und runterfährt), kann es zu weiteren Datenverlusten kommen. Das Filesystem beginnt direkt damit, die freigewordenen Blöcke wieder zu überschreiben. Grundsätzlich wird DD nur Dateien wiederherstellen können, für die es die entsprechenden Signaturen kennt. Das Programm muss über die gesamte Platte hobeln und anhand der Daten in den Blöcken erraten, um was für eine Datei es sich handeln könnte. Das funktioniert umso besser, je mehr Bezüge es zu den einzelnen Blöcken gibt. Bilder, Sound-dateien, Videos und alles was einen Header vor den jeweiligen Binärdaten hat resultieren in einem größeren Wiederherstellungserfolg.

Einfache Textdateien können hierbei schon problematischer sein oder Dateien die keinen strukturierten Aufbau haben. Auch können keine Dateien wiederhergestellt werden, deren Blöcke auf der gesamten Platte verstreut gewesen sind. Die Blöcke einer Datei müssen nacheinander auf der Platte geschrieben gewesen sein. War die Platte schon recht voll, werden gerade die letzten Daten sehr fragmentiert auf der Festplatte gelegen haben. Hier geht die Wahrscheinlichkeit der Rettung deutlich nach unten.

Vor allem darf man bei der Wiederherstellung auf keinen Fall als Zielort die Platte auswählen, auf der sich die gelöschten Daten befinden. Mit jeder wiederhergestellten Datei wird gleichzeitig weiterer Content gelöscht. Zur Datenrettung empfiehlt es sich immer die Platte sofort auszustöpseln und per Linux mittels "dd" eine Sicherungskopie der Platte anzulegen. Ich gehe hier so vor, dass ich mir eine virtuelle Maschine auf meinem VSphere Cluster anlege und die Platte mittels ssh auf eine virtuelle Platte klone. Danach lege ich einen Snapshot der virtuellen Kiste an und beginne dann mit der Datenrettung. Bei der Datenrettung von Journal-Filesystemen spielt es auch keine Rolle, unter welchem OS das getan wird. Da man hier einzelne Dateien aus den Rohdaten der Platte liest, kommt es hierbei drauf an wie gut das Programm ist, welches man zur Wiederherstellung einsetzt. Wir nutzen hier im Büro eine Software die durch mehrfache Wiederherstellung von Daten lernt und jedes Mal neue und eigene Signaturen anlegt.