OCTOSTOR

Die Octostor-Lösung im Detail

Daten-sicherheit mit der Octostor Backup-Lösung basiert auf den folgenden drei Säulen:

Lokationstrennung

Die Ablage von Backup- Daten an einem anderen physikalischen Ort ist zwingend, da im Falle eines Unglücks am Firmenstandort die Datensicherung nicht betroffen ist.
Die meisten kleinen und mittelständischen Unternehmen haben jedoch nur einen Standort und können somit die Datensicherung nicht an einen weiteren Standort auslagern.

Mit einem Backup in einen Cloud-Speicher erhält ein Unternehmen Zugriff auf einen zweiten Speicherort, der unabhängig von der Firmenlokation ist. Erst so entsteht echte Sicherheit für Unternehmensdaten!

Medienbruch

Cryptoviren oder auch Verschlüsselungstrojaner haben ihren Namen von der Funktion, die sie ausführen. Und diese Funktion ist leider nur negativ für die Betroffenen: Sie verschlüsseln Dateien mit dem Ziel einer Lösegeldforderung.

Die Viren / Trojaner gelangen meist über eine E-Mail ins System und kidnappen mit Hilfe von Verschlüsselungs-Algorithmen alle erreichbaren Dateien. Dann treten die Angreifer anonym auf das geschädigte Unternehmen zu und fordern ein Lösegeld in oft schmerzhafter Höhe. Fast alle Unternehmen sehen keinen anderen Ausweg, als das Geld zu bezahlen, in der Hoffnung, wieder Zugriff auf die Daten zu erlangen. Doch selbst die Zahlung stellt keine Sicherheit dar, so dass die Firmen doppelt geschädigt wurden:

- Verlust der Daten
- Verlust von Kapital

Das Problem für die meisten Unternehmen ist die Tatsache, dass auch das Backup, also die Versicherung ihrer Daten, über die gleichen Protokolle (Windows File Server Protokolle) erreichbar ist wie die Ausgangsdaten. Sind die Protokolle infiziert, bedeutet dies unter Umständen auch die Zerstörung des Backups. Ist dies der Fall, kann das unter Umständen die Existenz eines Unternehmens gefährden, da keinerlei Daten mehr verfügbar sind. Um dies auszuschließen, sollte ein Backup daher immer über ein anderes Protokoll geschrieben werden.

Bei der Backup-Lösung von Octostor wird das in der IT bereits etablierte und anerkannte SSH-Protokoll eingesetzt, denn es bietet zwei Vorteile:

- Verschlüsselung
- Dedizierte Authentifizierung notwendig

Ein Übergreifen des Verschlüsselungstrojaners auf dieses Backup ist damit nahezu unmöglich.

Versionssicherung

Die Sicherung läuft nach Bedarf täglich, wöchentlich oder ad hoc. Dabei werden nur Dateien gesichert, die im Vergleich zur vorherigen Sicherung verändert wurden. Dies spart:

- Bandbreite
- Sicherungszeit
- Speicher in der Cloud

Die Aufbewahrungszeit der gesicherten Dateien richtet sich nach der vom Kunden gewünschten Versionstiefe, die beim Einrichten des Sicherungsprofils definiert wird. Gegenüber herkömmlichen Backup-Konzepten bedeutet dies, dass nur die Dateien vom Backup gelöscht werden, welche diese definierte Generationstiefe erreicht und nicht die, die nur ein bestimmtes Alter überschritten haben. Zum aktuellen Sicherungszeitpunkt werden somit die Dateien gespeichert, die sich gegenüber dem letzten Sicherungszeitpunkt geändert haben.

Warum ist nicht das Alter, sondern die Versionstiefe wichtig?
Grundsätzlich interessieren bei Dateien meist nur die letzten Änderungen. Das Alter einer Datei wird somit nicht in Tagen oder Monaten gewertet, sondern in der Anzahl von Änderungen. Eine Datei, welche am Tag mehrfach verändert wird, ist nach ca. einer Woche bereits veraltet. Eine Datei hingegen, welche sich nur einmal im Monat ändert, ist nach einigen Wochen noch aktuell.