Backup

Hier erfährst du:

- Wie du dich (mit wenig Aufwand) für eine Backup-Lösung entscheiden kannst.
- Infos zum Thema Backup des Smartphones.
- Konkrete Anleitungen mit und ohne Backup-Programme.

Du solltest immer ein möglichst aktuelles Backup deiner Daten haben. Computer können kaputt werden, dein Gerät kann sich einen Virus einfangen oder deine Festplatte wird bei einer Hausdurchsuchung beschlagnahmt. Mit Backup meinen wir hier einfach mal nur, dass deine Daten nochmal woanders gespeichert sind. Dieses Backup sollte natürlich ebenfalls verschlüsselt sein. Wie du einen verschlüsselten Datenträger (zB eine Festplatte) erstellst, kannst du unter Aufbewahrungsverschlüsselung in diesem Wiki nachlesen.

Es gibt unterschiedliche Strategien, um die Daten zu sichern. Egal, ob die Daten im Hintergund automatisch übertragen werden oder du die wichtigen Daten händisch kopierst, am Anfang steht meist die Überlegung, welche Daten du überhaupt sichern musst. Auch solltest du dir überlegen, mehr als ein Backup anzulegen und eines der beiden an einem anderen Ort zu verwahren. Denn so ist bspw im Falle einer Hausdurchsuchung oder wenn deine Wohnung abbrennt, möglicherweise nicht nur dein Computer weg, sondern auch die Fesplatte auf der das Backup gespeichert ist. Damit du in so einem Fall trotzdem nicht deine Daten verlierst, kann es sinnvoll sein, die Daten noch woanders gespeichert zu haben. Ob du die Daten verschlüsselt in der Cloud oder auf einer verschlüsselten Festplatte bei einer Freund:in aufbewahrst, ist dabei egal.

Vorbereitungen und Überlegungen

Welche Daten möchte ich sichern?

Wie immer bei Sicherheitslösungen überlegst du dir zuerst, was du überhaupt für eine Lösung brauchst. Welche Daten möchtest du auf keinen Fall verlieren?

Wie wichtig ist dir beispielsweise die Sicherung von Browserverläufen, deines Chatverlaufes, deiner Programme oder dein Spielstand in einem Computerspiel? Im Sinne der Datenvermeidung als Sicherheitsstrategie ist auch zu empfehlen, dass nicht alles bis in alle Ewigkeit aufbewahrt wird!

Wir empfehlen, folgende Datengruppen bei einer Datensicherung zu berücksichtigen:

- Dateien, Dokumente, Fotos,... die dir wichtig sind
- E-Mail-Keys: vor allem dein privater Key, falls es dir wichtig ist, alte E-Mails lesen zu können
- Passwortmanager-Datenbank
- eventuell Programmdateien, wie Spielstände ...

Auf welchem Medium mache ich mein Backup?

- **Festplatte**: Du kannst deine Daten beispielsweise einfach auf eine externe Festplatte speichern, die widerrum natürlich auch verschlüsselt sein muss.
- **Cloud**: Falls du deine Daten auf eine Cloud speichern möchstest, solltest du unbedingt darauf achten, die Daten vorher auf deinem eigenen Gerät noch zu verschlüsseln. Denn du hast hier nicht mehr die alleinige Kontrolle über deine Daten, was diesen Punkt noch wichtiger macht.

Handy-Backup

Auch deine Handydaten wollen gesichert werden:

- Kontakte
- Dateien
- Fotos
- Programmdateien
- Signal,...

Hier ist es wohl am einfachsten das Handy am Computer anzustecken und die Daten regelmäßig händisch auf eine verschlüsselte Festplatte zu speichern.

Backup Strategien

DIY-Backup

Niemand sagt, dass automatisch auch immer leichter ist. Du kannst nämlich auch einfach die Ordner, die dir wichtig sind, selbst an den Sicherungsort kopieren. Dafür erstellst du einen neuen Ordner mit dem aktuellen Datum (z.B.: Sicherung_2021-01-31) auf deiner Sicherungsfestplatte und kopierst die relevanten Ordner von deiner Festplatte dort hinein. Wenn dir der Speicherplatz ausgeht, kannst du die ältesten Sicherungsordner löschen. Gerade wenn du keine riesen Datenmengen zu kopieren hast, ist dies sicher nicht die schlechteste Lösung.

Aus der Praxis: So mache ich mein DIY-Backup

Ich achte darauf, dass ich meine Daten schon sehr geordnet auf dem Computer ablege und nicht zu sehr verteile: Alles was mir wichtig ist, kommt in einen Ordner „Meine Dateien“. Darin finden sich dann die verschiedenen Unterordner „Dokumente“, „Fotos“, „Passwortmanager“, „Mein Email-Schlüsssel“ etc.

Meine externe 500GB-Festplatte mit USB-Anschluss habe ich mit Veracrypt verschlüsselt, die Anleitung dazu habe ich hier im Wiki gefunden.

Alle 1-2 Wochen stecke ich die externe Festplatte an, starte Veracrypt und gebe mein Passwort ein. Ich erstelle einen neuen leeren Ordner auf der externen Festplatte mit dem aktuellen Datum „Backup_2024-01-01“ und kopiere den Ordner „Meine Daten“ dort hinein. Das dauert ein paar Minuten. Mit Veracrypt wieder die Festplatte „aushängen/unmount“ und fertig.

Automatisiertes Backup

Automatisierte Backups haben einige Vorteile, jedoch müssen sie zuerst einmal eingerichtet werden. So kann ich zB Backupstrategien verwenden, die Speicherplatz sparen, indem sie nicht immer alle Dateien sichern, sondern sich nur merken, welche Daten seit dem letzten Backup verändert wurden und dann diese sichern. Außerdem muss ich so nicht immer selbst daran denken und es sollte im Hintergrund passieren. Hierfür gibt es unterschiedliche Programme, die dich dabei unterstützen können.

Anleitung Linux: Deja Dup

Deja Dup ist eine einfache Lösung für Datensicherung unter Linux:

Hier findest du eine bebilderte Anleitung für Deja-Dup/Datensicherung [en] wie du deine Datensicherung einrichten kannst.

Aber auch ohne Anleitung ist das Menu von Deja Dup sehr einfach gehalten und selbsterklärend:

- Unter „Zu sichernde Orte“ wählst du aus, welche Ordner du sichern möchtest. Alle Dateien und Unterordner in diesen Ordnern werden in die Datensicherung miteinbezogen.
- Unter „Zu ignorierende Orte“ kannst du (Unter-)Ordner auswählen, die du nicht sichern möchtest.
- Unter „Speicherort“ gibst du an, wo deine Sicherung abgelegt werden soll.
- Unter „Übersicht“ → „Jetzt sichern“ startest du das Backup. Oder du stellst unter „Zeitplanung“ den automatischen Vorgang ein. Vergiss nicht, - weil du ja ein verschlüsseltes! externes Speichermedium verwendest - dass du es vor dem Datensicherungsvorgang entschlüsseln musst.

Das Backup wird „inkrementell“ angelegt, das heißt, dass immer nur neu hinzugekommene oder veränderte Dateien auch neu am Ort der Datensicherung abgespeichert werden. Das spart nicht nur Zeit, sondern auch Speicherplatz.

Aus der Praxis: So kümmert sich Deja Dup automatisch um mein Backup
Ich wollte mich nicht schon wieder bei mir selbst rausreden, warum ich mich mal wieder nicht um meine Datensicherung gekümmert habe. Daher habe ich mich für eine (halb)automatische Lösung entschieden. Halbautomatisch darum, weil ich immer noch meine externe Festplatte anstecken und entschlüsseln muss - alles andere übernimmt ein Programm. Aber es hat mir trotzdem geholfen, dass ich nun regelmäßig meine Daten sichere.

Zuerst habe ich mir eine externe Festplatte besorgt und mit dem Programm *VeraCrypt* verschlüsselt. Wie das geht findet ihr als Anleitung zu VeraCrypt hier im Wiki.

Auch habe ich mir Deja Dup auf meinem Linux-Betriebssystem installiert und mit der Anleitung zu Deja Dup hier im Wiki eingerichtet. Da ich alle meine relevanten Dokumente und Fotos im meinem Home-Verzeichnis ablege, habe ich diesen Ordner als Quelle für das Backup angegeben. Da mir nicht wichtig war, dass das Downloadverzeichnis gesichert wird, habe ich im Programm ausgewählt, dass dieser Ordner bei der Datensicherung ignoriert wird, da ich gar nicht alles sichern möchte, was ich so runterlade.

Unter „Zeitplanung“ habe ich eingestellt, dass ich jede Woche meine Daten sichern möchte. Jetzt erinnert mich das Programm daran, weil es wöchentlich versucht die Daten zu sichern und dies auch dann, wenn ich die Sicherungsfestplatte gar nicht angesteckt habe. Die Sicherung schlägt dann zwar fehl, da ja die Festplatte fehlt, aber ich werde daran erinnert, das Backaup zu machen: Ich stecke die Platte an, entschlüssel sie mit VeraCrypt und starte die Datensicherung.

Anleitung Windows: Backup

Fix Me! - Dieser Artikel muss noch geschrieben werden.

Anleitung MAC: Backup

Fix Me! - Dieser Artikel muss noch geschrieben werden.

Zum Weiterlesen

Backupstrategien in englischer Sprache | Backupstrategies Security in-a-Box [english]