

Wie sicher ist ein verschlüsseltes Time Machine Backup ?

Beitrag von „AgentUgly“ vom 18. März 2021, 16:22

Hallo zusammen,

zur Abwechslung mal eine allgemeine Frage zu Time Machine Backups.

Ich habe die Möglichkeit, auf einem NAS, das außerhalb meiner Wohnung steht, Backups anzulegen.

Bisher habe ich darauf nur "unsensible Daten" (Videos, Musik) gespeichert, aber würde es auch gerne als Speicher für meine TimeMachine-Backups

nutzen, weil ich dann nochmal eine externe Sicherung meiner Daten hätte, ohne diese in eine Cloud auslagern zu müssen.

Das finde ich eigentlich super, aber da es sich um persönlichen Daten handelt, bin ich noch vorsichtig.

Wenn ich auf dem für mich freigegeben NAS-Laufwerk ein verschlüsseltes Backup anlege, ist dann sichergestellt,

dass auch nur ich es entschlüsseln kann?

Das NAS wird nicht von mir administriert, deswegen kann ich nicht ausschließen,

dass andere Zugriff auf meine Daten haben (auch wenn es sehr unwahrscheinlich wäre).

Wenn das Backup jedoch so verschlüsselt wäre, dass nur ich es entsperren kann, könnte ich damit leben.

Wie ist Eure Meinung zu dem Thema?

Würde mich interessieren.. Danke vorab!

Beitrag von „ozw00d“ vom 18. März 2021, 16:50

machst halt ein verschlüsseltes tm backup, sehe das problem nicht. allerdings weiss ich nicht wies sich verhält. Aud em NAS wirst du wohl kein Admin sein.

Ob der Admin mit entsprechender Root berechtigung auf dem Speicherpfad dann Rechte bekommt habe ich bisher nicht ausprobiert, da bei mir Backups nur auf eigene Server kommen.

Theoretisch sollten die Daten allerdings in Verschlüsselter form vorliegen und nur mit dem Key in deiner Keychain entschlüsselt werden können.

Das Volume kannst du zusätzlich verschlüsseln, damit hättest einmal die daten und zusätzlich das Image welches auf dem Laufwerk liegt verschlüsselt.

Ob das nun 100% sicher ist, keine ahnung. Fakt ist jedoch kein System isst 100% sicher und wenn das zeug bei jemand anderem liegt, auch mist da deine daten nicht gebackupt sind.

Auf einem Nas ohne Ausfallsicherheit ist ein Backup mit TM auch nicht so dolle.

Besser du fährst eine Backup Strategie nach dem 3 Gen oder auch 3-2-1 Verfahren. so wie [hier](#) beschrieben.

oder eben so wie [hier](#).

Beitrag von „AgentUgly“ vom 18. März 2021, 17:01

Jo, Danke erstmal für die Antwort!

Ich mache regelmäßig TM-Backups auf externe Platten,

das hätte ich also sowieso noch.

Das Backup auf dem NAS wäre halt noch zusätzlich,
also eigentlich so wie bei der 3-2-1-Variante. Nur das es eben kein richtiges Cloud-Backup ist,
sondern auf dem NAS, das aber nicht bei mir zu Hause ist.

Also, wenn meine Bude unter Wasser steht und der Rechner + die Backup-Platte zerstört sind,
hätte ich diese Variante... 😊

Und wenn das verschlüsselte TM-Backup nur von mir geöffnet werden, alles super.

Beitrag von „EdD1024“ vom 18. März 2021, 18:46

So sicher wie das Passwort dazu ist. Allerdings wüsste ich nicht, dass auf dem Backup ein Brute-Force Schutz drauf ist. Also kommt jemand in den Besitz deiner Backups, hat er alle Zeit der Welt das Passwort zu knacken. Möglicherweise auch mit Rainbow Tables oder ähnlich.

Ich würde mich jedenfalls nicht sehr darauf verlassen, also keine existenzbedrohenden Geheimnisse darauf ablegen.

Beitrag von „Wolfe“ vom 18. März 2021, 19:12

Wenn das Time Machine Backup mit einem 128bit starken Schlüssel gesichert ist, dauert eine brute force Attacke etwa 1000 Jahre, bis AES geknackt ist.

Mir ist das sicher genug.

Beitrag von „pebbly“ vom 18. März 2021, 19:19

Im Zweifel gibt es Cryptomator etc. Dann werden die verschlüsselten Daten in TM gesichert und da diese wiederum auch verschlüsselt ist...

Beitrag von „AgentUgly“ vom 18. März 2021, 21:46

Ok, danke allerseits!

Das hilft mir auf jeden Fall weiter.

Ich werd das mal angehen und das TM-Backup ggf. ein bisschen vorsortieren.

Beitrag von „EdD1024“ vom 19. März 2021, 09:46

Das Passwort und der Verschlüsselungsalgorithmus haben miteinander nichts zu tun. Wenn Du als Passwort eine vierstellige PIN nimmst, kannst Du gerne auch mit weiß Gott was verschlüsseln....

Beitrag von „barrrrt“ vom 19. März 2021, 10:28

Wenn es eh schon unwahrscheinlich ist, dass jemand anderer auf das NAS zugreifen kann, dann würde ich ein verschlüsseltes Backup darauf ablegen.

Eine Überlegung in eine andere Richtung wäre auch: Wie groß ist die Wahrscheinlichkeit, dass dir jemand deine Backupplatten klaut und versucht dein TimeMachine Backup zu entschlüsseln? Denke da gibt es einfachere Wege an Daten zu kommen 😁

Und wenn das NAS nicht gerade von einem dubiosen Drogendealer oder gar Hacker stammt ... dann ist das Risiko schon verschwindend gering, oder?

Was mich noch interessiert: Das NAS ist also nicht in deinem Häusle, sondern ... sagen wir in einer anderen Stadt (also: WAN Strecke)? Wie greifst du denn auf das NAS zu für die Sicherung?

Beitrag von „Wolfe“ vom 19. März 2021, 10:38

„Das Passwort und der Verschlüsselungsalgorithmus haben miteinander nichts zu tun.“

<https://www.datenschutz.org/aes-verschluesselung/>

Passwortlänge und Sicherheit:

<https://www.1pw.de/brute-force.php>

Mein Passwort für das Time Machine Backup, das nicht zusätzlich von meiner nas verschlüsselt wird, besteht aus 36 Ziffern, Groß-Kleinbuchstaben und Sonderzeichen.

Ich fühle mich damit sicher.

Beitrag von „AgentUgly“ vom 19. März 2021, 13:01

[barrrrt](#)

...das NAS steht im Keller der Schwiegereltern und mit dem Admin bin ich verwandt 😊

Ich werd mal nachfragen, ob einer von denen vorhat, in Zukunft ins Drogengeschäft einzusteigen. Dann würde ich es mir nochmal überlegen 😊

Aber im Ernst: Ja, das Risiko ist gering, dass etwas nach außen gelangt. Ist ein sehr kleiner Personenkreis. Mir ging es wirklich mehr darum, dass die Daten privat bleiben und nur für mich

entschlüsselbar, weil es eben persönliche Daten sind, die nur mich betreffen.

Mein Gedanke war, dass ich das erste TM-Backup vor Ort mache (Ethernet), um den Datenhaufen einmal anzusammeln. Und dann die Änderungen entweder über Internet (VPN) oder übers WLAN, wenn ich da bin.

Beitrag von „barrrrt“ vom 19. März 2021, 13:16

[Wolfe](#) Jetzt weiss ich, dass ich nur Kennwörter mit einer Länge von 36 Zeichen bei dir überprüfen muss.....

Das "nur" müsste aber wohl in Klammern 😊

Übrigens eine ganz feine Funktion, wenn man Backups erstellen möchte, ist Hyper Backup mit einem Synology NAS.

1. Unterstützt so ein Synology NAS Time Machine
2. Hyper Backup sichert in die Cloud ODER auf andere Synology NAS. Wenn es eine andere NAS ist, hat der andere Admin keinen Zugriff auf den Sicherungscontainer.

[C2 Plan Synology](#)

Aber dafür bräuchte man natürlich ein Synology NAS + C2 Backupplan (wer allerdings ein Office 365 Account hat, kann auch zu Onedrive hochladen).

Der Beitrag ist jetzt aber nicht mehr ganz auf die hier gestellte Frage gemünzt, aber Backupstrategien find ich so oder so immer interessant. Sollte nur sicher UND einfach sein.... und ggfs. günstig....

Beitrag von „pebbly“ vom 19. März 2021, 13:28

Nur noch mal zur Sicherheit [AgentUgly](#) :

Time Machine kann nicht auf mehrere Datenträger den gleichen Speicherstand sichern. Verwendest du zwei gleichzeitig, müsstest du jedes Mal den Speicherort für das Backup ändern, schließt du die zwei abwechselnd an, haben sie unterschiedliche Speicherstände. Siehe <https://www.backblaze.com/blog...hard-drives-time-machine/>

Bei jedem Backup werden für veränderte Dateien Hardlinks gesetzt, was HDDs je nach Umfang gerne in die Knie zwingen kann - spätestens wenn automatisch alte Backups gelöscht werden. - Das Problem habe ich gerade.

Wenn du in ein Time Machine Backup rein schauen willst, lädt der gerne mal etwas, wegen der ganzen Links. Das über Netzwerk <Gbit dürfte sehr auf die Geduld gehen.

Beitrag von „AgentUgly“ vom 19. März 2021, 13:43

[pebbly](#)

Ja, das wäre für mich ok (also das Wechseln und die unterschiedlichen Speicherstände).

Mein regelmäßiges (wöchentliches) Backup bleibt die externe Platte,

auf dem NAS würde ich in unregelmäßigen Abständen "nach-sichern". Zeit spielt da eher eine untergeordnete Rolle, weil ich den Rechner da auch mal einen Tag stehen lassen kann.

Vom Speicherplatz her gesehen ändert sich wahrscheinlich nicht so viel, weil vor es allem Office-Kram ist(Dokumente, Mails, hin und wieder mal Bilder).

Aber wahrscheinlich muss ich es mal ausprobieren, um zu sehen, wie groß der Nerv-Faktor ist



Beitrag von „barrrrt“ vom 19. März 2021, 13:52

Du könntest sonst einfach regelmäßig das Backup vom externen Datenträger auf das NAS sichern.

Wie groß sind denn sonst deine wichtigen Daten? Alternativ: Zusätzlich zum Time Machine Backup (also in diesem Fall dann nur der externen Platte) diese Daten in OneDrive/GoogleDrive/etc. ablegen. Aber durch z.B. Boxcryptor verschlüsselt.

Beitrag von „Wolfe“ vom 19. März 2021, 16:04

„Time Machine kann nicht auf mehrere Datenträger parallel sichern.“

Mein Time Machine speichert auf mein nas und eine externe Festplatte.

Beitrag von „pebbly“ vom 19. März 2021, 17:06

Ich habe mich etwas undeutlich ausgedrückt und mal korrigiert.

Beitrag von „AgentUgly“ vom 19. März 2021, 18:14

[barrrrt](#)

Es wird wohl nicht mehr als ca. 200GB.

Und wenn die einmal auf dem NAS sind, sind die Änderungen durch Löschen oder neue Daten meist unter 1GB.

Beitrag von „ozw00d“ vom 20. März 2021, 12:47

[AgentUgly](#) wäre mir echt zu unsicher meine Daten in die Hände von jemanden zu geben der mir keine Garantie für etwaigen Ausfall geben kann (Backupstrategie, SLA).

Bei Diversen Cloudanbietern kann ich mich da rechtlich absichern, was zwar bei dem absolutem Worst Case (RZ wird in die Luft gejagt etc.) auch keine Garantie bietet.

Leider ist ein Backup immer nur dann auch Sicher wenn ich eine Kopie von der Kopie von der Kopie habe.

Ich möchte meine Daten einfach nicht in unfähige Hände legen, dein Nachbar ist kein offizieller Cloud anbieter oder Anbieter für Speicher / Backuplösungen? Dann finger weg davon.

Als Müllablage sicher praktisch (im Developement für Temporären schrott kram) oder zur auslagerung von irgendeinem kram den ich sowieso nicht benötige (naja kann man dann auch gleich löschen).

Nur als Beispiel: Du legst deine Musik Sammlung da ab und hast kein Backup (Systemausfall), dein nachbar hat nen Brand / drück weil ihm deine letzte reaktion nicht passte den löschen knopf. Wäre mir zu heikel.

Ursache für die meisten Datenverluste sind und bleiben Menschliches Versagen (nicht weit genug gedacht).

Nicht die Hardware, nicht der Datenträger.

Sind einfach zu viele Variablen die man bedenken muss.

Beitrag von „AgentUgly“ vom 22. März 2021, 20:47

Sorry, hat etwas gedauert. Generell würde ich Dir zustimmen, also wenns um ein professionelles Umfeld geht. Aber für mich als Privatmensch sind 2 Backups, von denen eins sogar noch räumlich getrennt ist, schon ein großer Zugewinn an Sicherheit.

Im Vergleich zu meinem bisherigen Backups auf externe Platten, die alle in einer Wohnung lagen, ist es auf jeden Fall ein Fortschritt, wenns vielleicht auch nicht perfekt ist.

Ich denke eher andersrum, dass viele Variablen zusammenkommen müssen, damit wirklich alle drei Speicherorte (Original, TM-Festplatte, NAS) unwiderbringlich hinüber sind. Ich denke, mit dem Risiko kann ich leben.

Der Admin des NAS ist im IT-Bereich tätig und wir sind tatsächlich verwandt 😊 Also auch da würde ich hoffen, dass der worst case nicht eintritt... weniger wegen dem Datenverlust, sondern aus persönlichen Gründen 😊

Wie gesagt, was ein professionelles Umfeld betrifft, in dem vielleicht Kundendaten betroffen sein könnten oder wichtige Geschäftsunterlagen, stimme ich Dir absolut zu.

Für den privaten Bereich, in dem es ja um sehr persönliche Daten geht, würde ich schon abwägen, ob ich diese in die Cloud geben möchte oder eine etwas unsichere, aber dafür selbstverantwortete Backup-Lösung wie z.B. das NAS nutze.

Einen schönen Abend und Danke für die Meinungen allerseits!