Erledigt HDD Verschlüsselung / Komfort gegen Sicherheit

Beitrag von „LL0rd“ vom 6. April 2019, 09:24

Hallo Leute,

ich brauche mal einen Rat von euch. Ich habe einen Desktop-Rechner mit OS X. In dem Rechner sind aktuell drei Platten. System SSD, eine Daten HDD und eine weitere SSD.

Die HDD und die zweite SSD sind mit OS X verschlüsselt. Also beim Formatieren wurde über das Festplattendienstprogramm die Verschlüsselung aktiviert. Allerdings wurde das Passwort wohl in der Keychain abgelegt, sodass der Rechner beim Booten nicht nach dem PWD fragt. Die System SSD ist offen. Nach 5 Min Abwesenheit fragt der Rechner nach einem Kennwort.

Nun gibt es folgendes Problem:

Zwar liegen viele Daten auf der verschlüsselten HDD, aber Meta-Daten wie z.B. der Browser-Verkauf, Cache Daten, etc. liegen alle unverschlüsselt auf der System-SSD. Soweit ich weiß, gibt es wenig Probleme mit Hackintosh und FileVault, ich weiß aber nicht, ob FileVault das Richtige für mich ist. Das aktuelle User-Passwort ist bei mir 8-Stellig, das für die anderen Platten über 30 Stellen lang. Was ich gerne hätte, wäre ein "Konzept" um den Rechner abzusichern. Also wenn er nach dem Ausschalten hochfährt, ich ein langes Passwort eingebe und wenn der Rechner zwischendurch gesperrt wurde, ich mit einem kurzen Passwort (oder anderen Credentials) den Rechner einfach entsperren kann.

Ich habe es unter Windows auch so mit TrueCrypt / Vera Crypt. Beim booten wird das lange TC-Passwort verlangt und bei der Nutzung ein kurzes Windows Passwort.

Und IMHO geht es bei nativen Macs ähnlich mit der Entsperrung mit der Apple Watch bzw. Fingerprint Sensor.

Gibt es auch so etwas für den Hackintosh?

Beitrag von „Thogg Niatiz“ vom 6. April 2019, 16:18

Mit einer geeigneten Airport Karte lässt sich ein Hackintosh einfach per Apple Watch entsperren. Ist sicher die eleganteste Lösung für dein Konzept.

Beitrag von „rubenszy“ vom 6. April 2019, 16:49

TrueCrypt gibt es auch für mac

https://sourceforge.net/projec...7.2-Mac-OS-X.dmg/download

veracrypt

https://www.veracrypt.fr/en/Downloads.html

Wenn ich das so lese, etwas paranoid oder hast vor wichtige Nutzerdaten zu sammeln, die das BKA nicht entschlüsseln soll.

Beitrag von „LL0rd“ vom 6. April 2019, 19:33

> Zitat von Thogg Niatiz
>
> Mit einer geeigneten Airport Karte lässt sich ein Hackintosh einfach per Apple Watch entsperren. Ist sicher die eleganteste Lösung für dein Konzept.

Hmm... Wirklich? Ich dachte, dass dieser zweite A5 (ich hoffe, dass es richtig ist) Chip benötigt wird, der nur im MBPr mit Bar verbaut ist. Heißt es, ich kann damit auch mein 13" MBPr ohne Bar entsperren?

> Zitat von rubenszy
>
> TrueCrypt gibt es auch für mac 
>
> Wenn ich das so lese, etwas paranoid oder hast vor wichtige Nutzerdaten zu sammeln, die das BKA nicht entschlüsseln soll. 

Ja, nur kann ich damit IMHO keine Systemplatte verschlüsseln. Oder doch? Ich habe aber evtl. eine Alternative gefunden. Das Home Verzeichnis ist im Netz per NFS freigegeben und wird dann beim Booten des Rechners eingehängt. Und auf dem NAS kann ich die Daten problemlos verschlüsseln. Das wäre die Alternative. Nur müsste ich hier ca. 300€ in ein 10 GBit Netz investieren. Was garnicht mal so viel wäre.

Und nein, es hat nichts mit irgendwelchen drei Buchstaben zutun, sondern mit 5: DSGVO. Bei einem Geschäftspartner wurde letztens eingebrochen und seine Rechner wurden geklaut. Jetzt erpresst man ihn damit die Daten zu veröffentlichen. Und da er Data Science auf Echten Daten betrieben hat, sind die Daten etwas kritisch.

Bei mir sind die Daten zwar verschlüsselt, aber mit meinen Metadaten, Cache, Browser History, etc. kann man - wenn man will - auch mir großen Schaden zufügen. Und darauf habe ich keinen Bock.

Beitrag von „Thogg Niatiz“ vom 6. April 2019, 19:39

> Zitat von LL0rd
>
> Hmm... Wirklich? Ich dachte, dass dieser zweite A5 (ich hoffe, dass es richtig ist) Chip benötigt wird, der nur im MBPr mit Bar verbaut ist. Heißt es, ich kann damit auch mein 13" MBPr ohne Bar entsperren?

Naja, mein Asus ROG Maximus VII Ranger hat sicher keinen SoC von Apple verbaut, wie auch immer der nun heißt. Aber seit ich die BCM943602CS drin hab kann ich mit der Watch den Desktop entsperren.

Beitrag von „svenatkins“ vom 6. April 2019, 19:39

Hab in meinem Hackintosh Bluetooth/ Airport Karte und kann mit Apple Watch entschlüsseln.

Das truecrypt nicht mehr als sicher eingestuft wird ist dir bewusst?

Beitrag von „Thogg Niatiz“ vom 6. April 2019, 19:47

> Zitat von LL0rd
>
> Und nein, es hat nichts mit irgendwelchen drei Buchstaben zutun, sondern mit 5: DSGVO. Bei einem Geschäftspartner wurde letztens eingebrochen und seine Rechner wurden geklaut. Jetzt erpresst man ihn damit die Daten zu veröffentlichen. Und da er Data Science auf Echten Daten betrieben hat, sind die Daten etwas kritisch.

Traurig, dass oft erst was passieren muss, bis sich die Leute bemühen mit den Daten. Das Problem ist nicht die GDPR - die ist nur ein rechtliches Hilfsmittel gegen die schwarzen Schafe. Gut, dass du dir vorher Gedanken machst

---

Beitrag von „rubenszy“ vom 6. April 2019, 19:59

@LL0rd Schon mal was von macOS to go oder Windows to go gehört?

Beitrag von „LL0rd“ vom 7. April 2019, 11:46

> Zitat von Thogg Niatiz

> Traurig, dass oft erst was passieren muss, bis sich die Leute bemühen mit den Daten. Das Problem ist nicht die GDPR - die ist nur ein rechtliches Hilfsmittel gegen die schwarzen Schafe. Gut, dass du dir vorher Gedanken machst

Je nachdem wie man es nimmt. Wenn die DSGVO dazu führt, dass sich einige Leute ein Geschäftsmodell daraus machen, Rechner zu stehlen um dann Firmen bzw. Personen zu erpressen, dann ist es schon ein Problem. Ich bin eh das Schwarze (Weiße) Schaf in unserer Straße, weil bei mir mittlerweile 7 Kameras am Haus hängen und Alarm schlagen, wenn jemand die Grundstücksgrenze übertritt. Die Verschlüsselung meines Home Directory soll nun die letzte Stufe des Schutzes sein. Denn ich kann nicht sicher gehen, dass die Programme, die ich einsetze nicht irgendwelche Temporären Dateien in mein Home-Verzeichnis schreiben.

Und ich möchte auch mich schützen, denn ich denke, dass jeder von uns in den vergangenen Monaten diesen SPAM bekommen hat von Wegen Rechner gehackt, Webcam aktiviert, beim W...xen aufgenommen. Wenn du nicht zahlst, schicken wir die Aufnahmen an Freunde.

> Zitat von rubenszy
>
> @LL0rd Schon mal was von macOS to go oder Windows to go gehört?

Nein. Und entweder bin ich grade immer noch zu müde oder ich habe tatsächlich nichts brauchbares gefunden. Ich dachte schon daran eine VM für produktive Arbeit aufzusetzen, aber das halte ich unterm Strich für nicht zielführend.

Beitrag von „rubenszy“ vom 7. April 2019, 12:03

macOS konnte man schon immer auf Sticks installieren, seit Windows 10 gibt es Windows to Go.

Heut zu Tage gibt es Sticks für 50 Euro die L und S von 400+MB/s haben, was völlig ausreicht.

Beitrag von „pebbly“ vom 7. April 2019, 13:23

Ich weiß nicht, wie stabil und zuverlässig die Partitionsverschlüsselung bei einem Hackintosh

ist. Ich denke der Ansatz mit der VM ist in deinem Fall der einfachste und sicherste Einsatz. Ich würde das mal mit einem Benchmark testen: Das Virtuelle Volumen der VM in einen TrueCrypt / Cryptomator (empfehle ich!) stecken und dann mal die Performance für deinen Einsatz testen. Der Vorteil ist, dass du eine komplett verschlüsselte Datei hast, die ohne Risiko gesichert und kopiert werden kann, aber im Zweifel sofort weg ist.

Beitrag von „rubenszy“ vom 7. April 2019, 14:09

Was der sicherste weg ist immer ein OS auf einem Stick den man bei sich träg, schön klein ist und im Notfall man ihn schnell zerstören kann, dazu noch ein komprimiertes Backup auf einen weit entfernten Server mit einer Time gesteuerten automatischen Löschfunktion.

Sicherer gehen deine Daten nicht.

Kurzes Beispiel laptop sieht scheiße aus, wenn du es versuchst auf der Straße zu zerschlagen, im Falle du bekommst es mit das sie es dir klauen wollen.

Hast du aber das wertvoll auf dem OS stick, können sie dir doch dein laptop klauen und was finden sie drauf, ein frisches unberührtes OS mit nichts wichtigem.

Außer du hinterlässt ihnen ein Ordner der halbwegs verschlüsselt ist, wo sie schon ein paar Tage brauchen um ihn zu knacken der dann ein paar Dateien enthält, die nicht von belang sind.

Beitrag von „LL0rd“ vom 7. April 2019, 14:42

Edit by al6042 -> Bitte keine Zitate von Beiträgen, welche direkt über deiner Antwort stehen...

Das ändert aber an dem Grundproblem nichts: Nämlich der Verschlüsselung.

Im Übrigen habe ich keinen einzigen Stick gefunden, der dauerhaft die Performance bringt. Der Sandisk Extreme Pro bzw. der Sandisk Extreme Go (also der Nachfolger) haben diePerformance nur eine sehr kurze Zeit gebracht, danach war es vorbei, da die Sticks zwar SSD-NAND verbaut haben, denen aber der Controller fehlt, der viele Aufgaben übernimmt.

Beitrag von „rubenszy“ vom 7. April 2019, 14:56

Was schwebt dir denn für eine Performance vor bei Meta-Daten.

Vorschläge hast du bekommen, mach das beste daraus viel Spaß, weil wenn ich das so lese, bekomme ich ganz komische Gedanken und das hat nichts mit Datenschutz zu tun.

Viel Spaß noch.