Erledigt Wie sicher ist ein Hackintosh?

Beitrag von „Apple-FanBoy1976“ vom 17. Mai 2017, 18:54

Hi Leute,

als Lehrling in der Hackintosh-Gemeinde sei mir diese simple, aber meiner Meinung nach doch wichtige Frage erlaubt. ich bin Mac-Benutzer seit 2014 und habe seit dem Abschied von Windows auch nichts vermisst 

Wie sicher ist ein Hackintosh-System, sowohl im Vergleich zu einem gekauften Mac, aber auch im Vergleich mit anderen Systemen z.B. Linux oder FreeBSD**?**

Also die grundlegenden Sicherheitsregeln(regelmäßige Backups, keine eMail-Anhänge öffnen und natürlich keine sogenannten "Möpse"-Seiten ansurfen) sind mir ja schon seit Windows-Tagen bekannt.

Wäre dankbar für Eure Meinungen und Anregungen um das System weiter zu härten.

Grüße aus Brandenburg an der Havel

Beitrag von „Nio82“ vom 17. Mai 2017, 19:07

Die Frage, Sicherheit Hacki vs Mac ist leicht beantwortet. Da auf beiden Rechner das selbe, im Fall unseres Forums, unveränderte MacOS läuft gibt es da keinen Unterschied. Was anderes ist es bei Distros wo "wir" in der Regel ja nicht wissen was alles daran verändert wurde.

In Bezug auf welches OS ist das sicherste, ist die Frage eigentlich relative. Den jedes OS hat seine Schwachstellen. Der Grund warum Windows gefühlt scheinbar soviel mehr hat ist, weil es

das am weitesten verbreitete OS ist weswegen sich die überwiegende Mehrheit der Schadware Programmierer auf dieses OS konzentrieren. Würde sich diese Marktdominanz durch MS ändern & zB Linux weiter verbreiten, würde man sicher auch da mehr "Schlupflöscher" finden, die dann prompt ausgenutzt werden. Sieht man ja auch an Android was auf Linux basiert.

P.S. Der menschliche Faktor darf dabei natürlich auch nicht außer acht gelassen werden. Den das beste OS nutzt nichts wenn der davor sitzende zu dumm, naive, oder ignorant ist & daher auf die einfachsten Fallen/Tricks reinfällt. "Brain.exe" (unter macOS -> "Brain.app") ist noch immer das allerbeste Antivirus Programm. 

Beitrag von „derHackfan“ vom 18. Mai 2017, 07:19

Btw: Ich habe diesen Thread mal in das passende Unterforum verschoben.

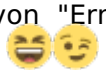
Beitrag von „Schorse“ vom 18. Mai 2017, 08:46

Nun es hat da schon ein paar nicht unwesendliche Unterschiede, da SIP und "nur verifizierte Entwickler" oft deaktiviert werden.
Ebenso FileVault nicht zu aktivieren empfohlen wird, da es im laufenden Betrieb eines Hackis recht tricky ist.
Bios als auch EFI sind im Original dicht!

Beitrag von „Thogg Niatiz“ vom 18. Mai 2017, 09:08

Die Diskussion gab es hier schonmal:
Neuerunge macOS Sierra, Sicherheit allgemein?

Beitrag von „Nio82“ vom 18. Mai 2017, 15:32

Nun die geänderte SIP Einstellung würde ich nicht als Unterschied ansehen. Es gibt auch genügend original Mac User die diese Funktion anpassen. Immerhin gibt es dazu genügend Anleitungen auf Mac Webseiten, ohne das es in Zusammenhang mit Hackintosh genannt wird.
Und was die FileVault angeht, diese bietet ja im Grunde nur Schutz für den Fall das der Rechner verloren geht, gestohlen wird oder von "Ermittlungsbeamten" einkassiert werden sollte. Warum auch immer diese das tun sollten? 

Und das auf "welches OS ist besser" bezogen, gibt es ähnliche Funktionen/Programme ja auch in/für die anderen OS z.B. TrueCrypt. Wie gut das dann wiederum bei den OS funktioniert steht natürlich auf einem anderen Blatt.

Beitrag von „Apple-FanBoy1976“ vom 18. Mai 2017, 21:32

Ich habe den Artikel mit den SIP Einstellungen sehr interessant gefunden und gleich mal bei mir geschaut. Hier war natürlich alles ausgeschaltet. Das habe ich jetzt umgestellt auf die erwähnte 0x3 Teil-entsperrt. Rechner neu gestartet und alles funktioniert wie gewohnt.

Beitrag von „Thogg Niatiz“ vom 18. Mai 2017, 22:14

Wie dort im weiteren Verlauf geschrieben - meine Systeme laufen sogar mit komplett aktivierter SIP (0x0). Ausprobieren solltest du das auch mal. Falls es nicht funktioniert, weil einzelne Kexts nicht geladen werden können, kannst du auch einfach wieder auf 0x3 oder eine ähnliche Konfiguration zurück.

Beitrag von „derHackfan“ vom 19. Mai 2017, 08:45

Bei mir steht in der config.plist immer 0x67 drin, über Sicherheit und Verschlüsselung, Updates oder Backups kümmere ich mich gar nicht, ob und wieviel Leichtsinn das ist, muss jeder für sich selber entscheiden.

Beitrag von „Doctor Plagiat“ vom 19. Mai 2017, 09:05

Bei mir steht auch 0x67 in der config. Ob das nun viel oder wenig Leichtsinn ist, wissen wahrscheinlich nur die die tief in der Materie drinstecken und genau einschätzen können wie groß und anfällig das geöffnete Tor ist.
Andere Faktoren spielen ja dabei auch noch eine Rolle, klicke ich ohne nachzudenken jeden Link in einer Webseite oder in einer E-Mail an, lade ich jede Software die ich irgendwo finde usw.
Das du dich über Sicherheit, Update und Backups gar nicht kümmerst, finde ich schon wieder grob leichtsinnig, vielleicht sogar fahrlässig. Aber wie du ja schon geschrieben hast, muss das jeder für sich selbst entscheiden.

Beitrag von „Schorse“ vom 19. Mai 2017, 14:07

Wer mit 0x67 unterwegs ist kann sich das Tool einmal ansehen und eventuell nutzen.
Die weiteren Tools des Erstellers sind auch sehr gut.

RansomWhere?

Beitrag von „griven“ vom 23. Mai 2017, 23:19

@Doctor Plagiat wie weit das Tor geöffnet ist oder nicht hängt immer vom Intellekt dessen ab der vor dem Rechner sitzt

Die SIP ist für sich genommen eine gute Sache denn sie schützt das System vor ungewollten und gewollten Änderungen sprich Systemdateien sind per se nicht mehr veränderbar für den Betrieb auf einem MAC mit dem was Apple dem User zugesteht sicher eine tolle und sichere Sache für Individualisten eher eine Katastrophe. OS-X war auch vor der SIP schon relativ sicher

denn der Gatekeeper lässt das ausführen von nicht signierter Software in der Regel auch ohne SIP nicht zu es sei denn man gibt ihm explizit die Anweisung dazu und selbst dann ist in den meisten Fällen noch die Eingabe des Passworts fällig...

Wer nicht vollkommen gegen den Bretterzaun gerannt ist sollte auch ohne SIP mit OS-X einigermaßen sicher unterwegs sein alle anderen kaufen sich besser einen MAC und lassen die Finger von der SIP 

Beitrag von „Doctor Plagiat“ vom 24. Mai 2017, 14:34

> Zitat von griven
>
> wie weit das Tor geöffnet ist oder nicht hängt immer vom Intellekt dessen ab der vor dem Rechner sitzt

Das habe ich doch indirekt auch geschrieben. Ich zitiere mich mal sebst:

> Zitat
>
> Andere Faktoren spielen ja dabei auch noch eine Rolle, klicke ich ohne nachzudenken jeden Link in einer Webseite oder in einer E-Mail an, lade ich jede Software die ich irgendwo finde usw.