

Erledigt

macOS als leichte(re)s Ziel für Malware

Beitrag von „blackcat“ vom 11. August 2019, 18:09

Mac-/Hackintosh-User sind demnach die leichteren (und lohnenswerteren) Opfer als Win(10)-User:

<https://m.spiegel.de/netzwelt/...-zu-hacken-a-1281361.html>

Beitrag von „revunix“ vom 11. August 2019, 18:34

Einfach sein Hirn einschalten, dann bekommt man auch nichts...

Unter Windows hatte ich schon über 10 Jahre keine Viren mehr gehabt.

Beitrag von „Doctor Plagiat“ vom 11. August 2019, 18:48

Es geht hier aber nicht um "Hirn einschalten" sondern um Sicherheit der Betriebssysteme, also wie leicht bzw. schwer sind sie angreifbar und wie schnell können Sicherheitsmechanismen ausgehebelt werden.

Beitrag von „Achilles31“ vom 11. August 2019, 19:15

Das Problem meiner Meinung nach ist dass jeder User denkt er braucht unbedingt den Root bzw. Administrator Zugriff.

Ich persönlich nutze seit fast 10 Jahren in der Windows Welt den normalen "Benutzer" - sollte Admin benötigt werden um etwas zu installieren schalte ich halt kurz um bzw. mache ein "ausführen als".

Im MacOS gibt es ähnliche Möglichkeiten - nur nutzen muss man sie

Update:

Bitdefender für MacOS rockt - ich liebe es 😊

Beitrag von „Cortablo“ vom 11. August 2019, 20:18

Was ich extrem krass finde ist das unter macOS die Firewall Standardmäßig deaktiviert ist.

Beitrag von „ResEdit“ vom 11. August 2019, 20:41

Da liegen noch eine Reihe mehr Dinge im Argen, wenn man es ganz genau nehmen will. Ich empfehle diese Blogs, um sich in das Thema einzulesen: <https://blog.bejarano.io/hardening-macos.html>

(der ist zwar nicht top-aktuell, allerdings recht solide, was die Grundlagen betrifft) Und dann noch den hier: <https://objective-see.com/blog.html> (der dürfte allgemein bekannter sein und wird auch regelmäßig aktualisiert).

Wer auf der Suche nach einer guten Quelle in unserer Landessprache ist, wird hier fündig: <https://www.kuketz-blog.de/tsc...ke-ein-leben-ohne-google/>

Beitrag von „ozw00d“ vom 11. August 2019, 21:13

richtig gut beschrieben um u.a. das os abzusichern gibt es hier <https://github.com/drduh/macOS-Security-and-Privacy-Guide>

ich hab außerdem clamav am laufen (die kostenfreie version) welche im wöchentlichen abstand das system und alle verbundenen platten scannt.

dazu brain-2.0.app und alles ist tutti.

Beitrag von „herrfelix“ vom 12. August 2019, 09:55

Patrick Wardle, der im oben verlinkten Artikel interviewt wird, betreibt übrigens auch die Seite objective-see.com

Beitrag von „blackcat“ vom 12. August 2019, 13:05

Genau das ist der Grund, warum ich das hier gepostet hatte, [revunix](#) - auch ich habe mich viel zu lange darauf verlassen, dass mir auf dem Mac/Hackintosh nix passieren könne.

Schon allein deshalb, weil sich durch die geringe Reichweite das für keine Cyberkriminellen lohnen würde.

Das ist aber schon lange nicht mehr so. Es gibt heute viel mehr Mac-User als vor 20 Jahren. Und in dem Artikel wird ja auch recht plausibel erklärt, dass sich gerade die Zielgruppe sehr lohnt, weil sie aus Leuten mit viel Geld und Verantwortung bestünde.

Ich jedenfalls verlasse mich nicht mehr darauf, mit Applesystemen immer auf der sicheren Seite zu sein.

Beitrag von „Tomis“ vom 15. August 2019, 18:30

[Zitat von blackcat](#)

Mac-/Hackintosh-User sind demnach die leichteren (und lohnenswerteren) Opfer als

Win(10)-User:



na... ja... sieht aber eher nach dem hier aus...

Microsoft warnt vor Sicherheitslücken bei Windows 10 sowie zwei weiteren Betriebssystemen. Das Unternehmen fordert Nutzer nun in einer Mitteilung auf, ein neues Update sofort zu installieren und das Betriebssystem zu aktualisieren.

Quelle: <https://www.netzwelt.de/betrug...indows-so-schliessen.html>

Beitrag von „mhaeuser“ vom 15. August 2019, 22:52

Was kommt als nächstes, leeres Adminpasswort? Ach, wuuuups