Erledigt Die liebe Sicherheit

Beitrag von „kuckkuck“ vom 21. Januar 2016, 07:43

Hey guys!
Ich habe ein paar wirre Gedanke durch den Kopf gehen gehabt bezüglich Sicherheit, vielleicht könnt ihr mich ja da aufklären
1. Ich habe mich gefragt wie sensibel die Daten in diversen DSDTs und Configs sind die hier Tag ein Tag aus gepostet werden. Ich habe mich gefragt ob es möglich ist das fremde Personen auf diese Dateien zugreifen oder ob unser Forum diese ausreichend beschützt, bitte nicht falsch verstehen ;/
2. Außerdem habe ich mich noch etwas bezüglich Sicherheit mit OS X gefragt: Vor der Installation von Kexten und anderen Dateien müssen häufig Sicherheitfeatures von OSX umgangen oder beseitigt werden (zB: System Integrity Protection und der Developer Mode im Terminal) daraufhin habe ich mich gefragt, wie sicher ist denn unser schönes OS X (El Capitan) danach noch nach außen hin? OSX kommt ja von Haus aus mit einigen schönen Sicherheitsfeatures weshalb ich auch noch nie Probleme mit Viren hatte und das seit dem Powerbook G4 Titanium. Aber wie siehts da aus mit Hackintoshs? Wird durch die Veränderung des systems die wir betreiben unsere Sicherheit gefährdet?
Ich hoffe ihr könnt mich aufklären

Beitrag von „al6042“ vom 21. Januar 2016, 08:10

Zuerst werfen wir mal den doppelten Thread raus.

Sowohl die DSDTs als auch die Config.- oder Defaults.plist enthalten keine personenbezogenen Daten.
Darin stehen auch keine Angaben über die tatsächlich genutzte Hardware.
Zusätzlich wurde vor wenigen Tagen die Kommunikation zum Forum auf HTTPS-Verschlüsselung geändert.
Somit sehe ich hier kein Problem.

Das Öffnen von Systemen per umgehen der SIPUtility, bzw. der Nutzung von "Rootless" oder "Kext-dev-mode", sollte für Hackintoshler eigentlich kein Problem darstellen.

Diese Funktionen werden benötigt um den Hacki überhaupt zum Leben zu erwecken... eine Situation, die einem realen Mac nicht passieren sollte.
Das wiederum geht aber einher mit der Tatsache, das die Leute hier diese Funktionen bewusst nutzen.
Genauso bewusst sollten sie natürlich auch im Umgang mit fragwürdigen Programmen oder Webseiten sein, was aber auch für alle Betriebssysteme gilt.
Kein System ist 100%-ig sicher... ausser du schaltest es nie ein.

Beitrag von „Sascha_77“ vom 21. Januar 2016, 08:50

Und bzgl. Viren noch die Anmerkung, dass es weniger an der "Sicherheit" von OS X liegt (Lücken gibts auch hier) sondern an der Tatsache das Virenprogrammierer das System nicht wirklich als lohnendes Ziel sehen. Die meisten Unternehmen & Co. haben Windowsnetzwerke.

Beitrag von „Kazuya91“ vom 21. Januar 2016, 09:06

Ein OSX ohne SIP ist trotzdem tausend mal sicherer als ein Windows.

Beitrag von „Monchi_87“ vom 21. Januar 2016, 09:09

Zumal man nach dem injecten der benötigten Kexte SIP wieder komplett aktivieren *kann*, wenn man es möchte!

Beitrag von „Sascha_77“ vom 21. Januar 2016, 09:23

> Zitat von Kadir91

> Ein OSX ohne SIP ist trotzdem tausend mal sicherer als ein Windows.

Ja zumindest solange bis der User nicht blind jeder Aufforderung nachkommt sein Adminpasswort einzugeben ohne zu wissen warum das plötzlich benötigt wird. Aber das ist dann eher wieder das meistverbreitete Problem: Das größte Sicherheitsrisiko sitzt vor dem Bildschirm.

Von daher ist es gar nicht so schlecht, dass OS X nicht den Beliebtheitsgrad/Verbreitung wie Windows hat. Da ist man nicht wirklich gefährdet. Und ich hoffe, dass ich auch in ein paar Jahren noch ohne Antiviren-Software mein System relativ gefahrlos betreiben kann.

Beitrag von „kuckkuck“ vom 21. Januar 2016, 16:19

Danke für die ganzen Nachrichten! Das der Threat zweimal geöffnet wurde ist ja komisch, ich habe ihn ja nur einmal geschrieben. Gut zu wissen das alles bedenkenlos ist, solang das Problem nicht hinter dem Hacky sitzt

---

Beitrag von „mhaeuser“ vom 21. Januar 2016, 17:48

Jeder, der so sicher ist, dass OS X wie eine Burg steht, sollte sich mal fragen, wie es denn sein kann, dass Clover und Ozmosis trotz aktiviertem KASLR (slide) an den Kernel kommen und dessen Erweiterungen patchen können.

Beitrag von „kuckkuck“ vom 21. Januar 2016, 19:33

Ja das ist klar dass auch OSX seine Lücken hat, aber im Vergleich zu anderen Betriebssystemen ist OSX auch dank UNIX ganz vorne dabei

Beitrag von „mhaeuser“ vom 21. Januar 2016, 19:46

Was an OS X is denn wirklich (noch) UNIX?

Beitrag von „kuckkuck“ vom 21. Januar 2016, 19:50

Da fragst du den falschen

Beitrag von „Sascha_77“ vom 21. Januar 2016, 20:47

> Zitat von Download-Fritz
>
> Was an OS X is denn wirklich (noch) UNIX?

Na der Darwin-Unterbau natürlich.

Beitrag von „mhaeuser“ vom 21. Januar 2016, 21:15

Natürlich? Also von einem System, dessen Kernel 'X is Not UNIX' heißt, erwarte ich nicht allzu viel...

Beitrag von „griven“ vom 21. Januar 2016, 22:06

Tief im inneren von OS-X ist schon noch einiges an Unix vorhanden denn letztlich basiert Darwin schon noch auf FreeBSD. Interessant wird es beim Kernel denn der XNU Kernel von OS-X ist ein Hybridkernel zusammengebaut aus dem MachKernel,dem FreeBSD Kernel und weiteren Anteilen.

> Zitat von "WikiPedia"
>
> XNU ist ein hybrider Kernel, bestehend aus Teilen des Mach-3.0-Mikrokernels und des monolithischen FreeBSD-Kernels, aber auch aus Teilen von MkLinux, NetBSD und OpenBSD.[3] Der XNU-Kernel von Darwin Version 7 entspricht dabei dem FreeBSD-Kernel in Version 5.[4]

Der BSD Teil kümmert sich hierbei um das Mehrbenutzersystem, den TCPIP Stack, die Synchronisierung und Steuerung von Prozessen während sich der Mach Teil für Multitasking, Speicherverwaltung und Fehlerbehandlung verantwortlich zeichnet. Flankiert wird das ganze vom I/O Kit welches sich um Plug and Play, Hotplugging sowie das Energiemanagement und die Extensionsverwaltung kümmert (I/O Kit Bestandteile sind bis heute schön zu erkennen z.B. IOUSBFamily.kext usw...). Demnach stimmt es schon X is Not Unix wobei es hier wohl richtigerweise heißen müsste X is Not (only) Unix