

Erledigt SIP für Anfänger

Beitrag von „markquark“ vom 29. Januar 2017, 21:52

Seit OS X Yosemite müssen Kernel-Erweiterungen, wie z.B. Treiber -Kexte, signiert sein. OS weigert sich zu booten, wenn unsignierte Erweiterungen vorhanden sind.

[SIP](#) umfasst eine Reihe von Mechanismen, die durch den Kernel erzwungen werden. Ein Herzstück ist der Schutz der System-

Dateien und Verzeichnisse gegen Änderungen durch Prozesse ohne eine bestimmte "Berechtigung", auch wenn sie vom Root-Benutzer oder einem Benutzer mit Root-Rechten (sudo) ausgeführt werden.

Apple sagt, dass der Root-Benutzer ein erheblicher Risikofaktor für die Sicherheit des Systems sein kann. Hahaha.

Besonders auf Systemen mit nur einem einzigen Benutzerkonto, auf denen dieser Benutzer auch der Administrator ist. Hahaha.

[SIP](#) ist also standardmäßig aktiviert.

Und jetzt kommen wir zur der Frage: **Wie ist das überhaupt mit dem [SIP](#) bei den hackintosh-Rechnern?**

Um ein macOS auf einen hackintosh zu kriegen müssen Kernel-Erweiterungen geladen werden, die nicht signiert sind,

was Apple aus irgendeinem seltsamen Grund nicht machen will. Um das zu schaffen muss Clover [SIP](#) deaktivieren.

Das Deaktivieren wird durch die config.plist angezeigt und gesteuert.

Bei jedem hackintosh mit OS X 10.10-10.12 ist [SIP](#) teilweise oder vollkommen deaktiviert.

Geben wir im Terminal den Befehl: `csrutil status`

Es kommt z.B. folgendes (ist Clover default):

[System Integrity Protection](#) status: enabled (Custom Configuration).

Configuration:

Apple Internal: *disabled*

Kext Signing: *disabled*

Filesystem Protections: *disabled*

Debugging Restrictions: *enabled*

DTrace Restrictions: *enabled*

NVRAM Protections: *enabled*

This is an unsupported configuration, likely to break in the future and leave your machine in an

unknown state.

Öffnen wir die config.plist mit Clover Configurator 2, Clover Configurator > Rt Variables > BooterConfig und CsrActiveConfig

steht unter CsrActiveConfig: 0x3, was bedeutet: [SIP](#) Partially Disabled (Loads unsigned kexts).

Unter BooterConfig: 0x28, und das ermöglicht zusätzlich dem Clover die Injektionen beim booten.

Diese Einstellung haben vermutlich die meisten.

CsrActiveConfig ist eine IOReg-Eigenschaft, Bootloader stellt den Wert von [SIP](#) ein.

Clover steuert also [SIP](#). Je grösser die Zahl nach x, desto weniger bleibt von dem [SIP](#).

Die häufigsten Einstellungen auf einem echten mac sind:

0x0 = [SIP](#) Enabled (Default)

0x3 = [SIP](#) Partially Disabled (Loads unsigned kexts)

0x67 = [SIP](#) Disabled completely

Hoffentlich stimmt das was ich da schreibe. Hahah.

Beitrag von „derHackfan“ vom 29. Januar 2017, 22:00

Du könntest noch 0x7F hinzufügen, aber ansonsten ist das doch ein alter Hut mit der [SIP](#) ... 😄

Beitrag von „markquark“ vom 29. Januar 2017, 22:17

Ist doch für Anfänger nicht für dich.

Beitrag von „mhaeuser“ vom 29. Januar 2017, 22:36

[Zitat von markquark](#)

Clover steuert also [SIP](#). Je grösser die Zahl nach x, desto weniger bleibt von dem [SIP](#).

Öhhmmm... nein, das ist eine Bitmaske. 😊

Beitrag von „markquark“ vom 29. Januar 2017, 22:38

Was ist und macht eine Bitmaske?

Beitrag von „mhaeuser“ vom 30. Januar 2017, 00:08

<https://de.wikipedia.org/wiki/Bitfeld>

Jedes Bit hat eine eigene Funktion, der Zahlenwert ist kein "Level".

[Zitat von markquark](#)

Bei jedem hackintosh mit OS X 10.10-10.12 ist [SIP](#) teilweise oder vollkommen deaktiviert.

Ich hab' [SIP](#) vollkommen aktiviert...

Beitrag von „Thogg Niatiz“ vom 30. Januar 2017, 08:11

Ich habe auf meinen Systemen ebenfalls die [SIP](#) komplett aktiviert. Da alle erforderlichen Änderungen am System durch Clover durchgeführt werden, ist das gar kein Problem.

Beitrag von „MacGrummel“ vom 30. Januar 2017, 08:29

Man muß eben nur beim ersten Start die [SiP](#) zumindest teilweise abschalten, wenn nicht alle neuen Kexte in den Clover-Ordern untergebracht sind. Wenn unsere Hackintosh-Kexte erstmal im Cache sind, kann die [SiP](#) auch durchaus voll "an" auf 0x0. Das gilt übrigens auch für echte Macs, wenn man die Webdriver für moderne(re) Nvidia-Maxwell- Grafikkarten nutzen möchte. Ein Mal auf "aus"(0x3 reicht aus), starten und die Kexte laden, danach wieder auf "an".

Beitrag von „markquark“ vom 30. Januar 2017, 09:19

>>> MacGrummel

Na diese Information hab ich gesucht. Man will doch keinen weniger sicheren hackintosh PC haben als die echten macs.

Die zweite Sache war es, wie man [SiP](#) auf 0x0 umschaltet. Ob es reicht im Clover Rt Variables > BooterConfig und CsrActiveConfig auf 0x0 einzustellen.

Da hat mir jemand über Bitmaske erzählt, und so genau will ich das nicht wissen. Sogas würde ich gerne den Binärzahlenschubser überlassen.

Ich will nur wissen, ob es tatsächlich Wirkung hat auf [SiP](#) im OS. Werde ich heute noch testen.

Ich will Vollständige Sicherheit von dem OS eingeschaltet haben.

Ist doch keine schlechte Idee, oder?

OK ausprobiert. Tatsächlich, Änderung in Clover hat Einfluß auf OS X. Habe beide Werte auf 0x0 eingestellt. [SiP](#) ist voll "enabled". Probleme habe ich keine festgestellt.

So sparrt man sich das booten der Recovery. Dieses Programmchen SIPUtility funktionierte bei mir nicht. Nach einstellen eines Wertes gab es error. Den Zustand kann man aber überprüfen.

Man kann beide Werte auf 0x0 einstellen, aber bevor man irgendwas mit dem System macht, sogar [Rechte reparieren](#), sollte man wieder den Standard wiederherstellen.

CsrActiveConfig: 0x3, BooterConfig: 0x28. Sonst kann es passieren, dass OS X nicht startet.

Achtung!

Spiel mit [SIP](#) hat mit sound abgeschossen. Ktext lässt sich nicht installieren. Hat mich Stunden Arbeit gekostet.