

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.