Erledigt Neuerunge macOS Sierra, Sicherheit allgemein?

Beitrag von „Lisa“ vom 25. September 2016, 12:23

Hallo,
in Sierra stehen in Sicherheit-Allgemein nur noch zwei Auswahlmöglichkeiten zur Verfügung.
- App Store
- App Store und verifizierte Entwickler

Bei OS xEl Capitan konnte man noch (- Keine Einschränkung) auswählen.

Ist der Wegfall von (- Keine Einschränkung) ein Nachteil bzgl. installieren von unsignierter Software?

Schöne Grüße

Beitrag von „Patricksworld“ vom 25. September 2016, 12:32

hallo. Versuche doch einmal

Code

1. sudo spctl --master-disable

in das Terminal einzugeben

Beitrag von „Thogg Niatiz“ vom 25. September 2016, 20:30

Prinzipiell ist es kein Nachteil, dass man "Keine Einschränkungen" nicht mehr auswählen kann. Theoretisch kann es durch diese Option nämlich schneller mal passieren, dass irgendeine ungewünschte Software ausgeführt wird. Ich persönlich habe es seit Yosemite nicht verstellt, da es zumeist reicht, ein un-/fremdsigniertes Programm via Rechtsklick > "Öffnen" zu starten und einmalig zu bestätigen, dass man es tatsächlich öffnen will. Für jeden halbwegs normalen User, insofern man das in der Hackintosh Community sagen kann , reicht dieser Weg vollkommen aus. Die Option "Keine Einschränkungen" sehe ich erst als relevant an, wenn jemand entwickelt und/oder mehrere dutzend neue Programme am Tag startet - und für diesen Fall gibt es obige Einstellung der spctl

Bei besonders hartnäckigen unsignierten Programmen, die angeblich beschädigt sind und auch nicht per Rechtsklick öffnen lassen wollen hilft dieser Befehl, um ebenfalls eine Ausnahmeregelung für das einzelne Programm zu erstellen:

Code

1. sudo xattr -rd com.apple.quarantine /path/to/application.app

Es gibt also fast keinen Grund, Gatekeeper zu deaktivieren, das genau wie die SIP eine elementare Sicherheitsfunktion in macOS darstellt - diese sollten ja nicht permanent deaktiviert bleiben

---

Beitrag von „jboeren“ vom 26. September 2016, 10:34

Welchen wert soll man bei sip wählen?

Beitrag von „Thogg Niatiz“ vom 26. September 2016, 11:21

Bei den meisten wird es ausreichen, Teile der SIP zu deaktivieren, damit unsignierte Kexts

geladen werden können. In Clover ist das folgender Wert:

Code

```
1. <key>CsrActiveConfig</key>
2. <string>0x3</string>
```

0x0 aktiviert die SIP und 0x67 deaktiviert sie vollständig, letzterer Wert sollte aber nur beim Experimentieren und in Ausnahmefällen dauerhaft verwendet werden.

Beitrag von „Schorse“ vom 26. September 2016, 17:45

Hmm, ich kann nicht booten wenn ich nicht 0X67 eingestellt habe!
Bei 0x3 KP, bei 0X0 sowieso KP

Beitrag von „Thogg Niatiz“ vom 26. September 2016, 18:04

Dann darfst du dich zu den Ausnahmen zählen. Übrigens klappt es bei meinem Notebook auch nur mit vollständig deaktivierter SIP ohne Kernel Panics.

Beitrag von „Schorse“ vom 26. September 2016, 18:33

Und dabei habe ich nur die Fakesmc, LAN und Sensorenkexte am Start. Kann ich das noch irgendwie beeinflussen?

Beitrag von „Thogg Niatiz“ vom 26. September 2016, 18:55

Mein Tower verwendet auch FakeSMC.kext, IntelMausiEthernet.kext, die Sensoren und außerdem AppleALC.kext, bootet problemlos mit 0x3:

Code

1. $ csrutil status
2. System Integrity Protection status: enabled (Custom Configuration).
3.
4.
5. Configuration:
6. Apple Internal: disabled
7. Kext Signing: disabled
8. Filesystem Protections: disabled
9. Debugging Restrictions: enabled
10. DTrace Restrictions: enabled
11. NVRAM Protections: enabled
12. BaseSystem Verification: enabled

Alles anzeigen

Edit: Der Tower und auch mein Notebook booten sogar mit 0x0 ohne Probleme

Welche LAN Kext verwendest du denn und hast du zusätzlich irgendwelche Änderungen in /S*/L*/E* ? Bei mir ist dort alles Vanilla - die Kexts können alle von Clover injiziert werden. Wahrscheinlich hast du in /S*/L*/E* für den Soundchip irgendwas modifiziert, da du oben nichts dergleichen aufgeführt hast. Dann ist es wahrscheinlich Zeit, auf die AppleALC.kext umzusteigen.

Beitrag von „Schorse“ vom 26. September 2016, 19:24

Hmm..
Nein in /S*/L*/E* habe ich nichts eingefügt oder verändert. Sound erhalte ich über eine USB Soundblaster.

Wenn ich von meinem USB Clover Bootstick starte kann ich ohne weiteres x03 wählen und der Rechner startet.
Von der EVI jedoch KP 😕

Beitrag von „jboeren“ vom 26. September 2016, 20:09

wie kann man bei Ozmosis die sip einschalten? laut csrutil ist sie disabled...

Beitrag von „Thogg Niatiz“ vom 26. September 2016, 20:13

@Schorse
Da weiß ich momentan leider auch nichts...

@jboeren
Das kannst du mit Ozmosis im Terminal machen, wenn du in die Recovery Partition bootest. Dort kannst du mit dem Befehl csrutil die einzelnen Parameter für die SIP ändern.

Beitrag von „griven“ vom 29. September 2016, 23:48

Alternativ geht es aber auch über die Defaults.plist

Code

```
1. <key>Defaults:7C436110-AB2A-4BBB-A880-FE41995C9F82</key>
2. <dict>
3. <key>csr-active-config</key>
4. <integer>127</integer>
5. </dict>
```

oder aber über den NVRAM mit

Code

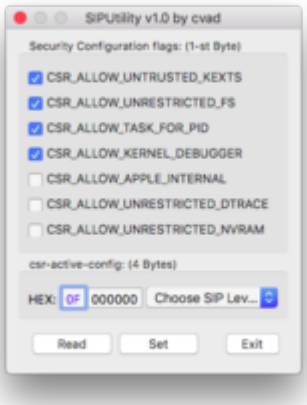
```
1. sudo nvram 7C436110-AB2A-4BBB-A880-FE41995C9F82:csr-active-config=0x7F
```

Beitrag von „jboeren“ vom 30. September 2016, 07:51

Welche funktion entspricht den wert 127 / x0F ?
Oben wurde x03 diskutiert.

Beitrag von „Thogg Niatiz“ vom 30. September 2016, 08:01

0xF erlaubt noch ein wenig mehr als 0x3:



Beitrag von „jboeren“ vom 30. September 2016, 08:09

Cooles utility! Das macht vieles einfacher!!