Erledigt Kann SIP nicht aktivieren

Beitrag von „Banduri1984“ vom 31. Juli 2017, 19:21

Hallo Leute

Mein Laptop ist fast fertig.
Einer meiner letzten Probleme ist das ich SIP nicht aktivieren kann.

Unter CsrActiveConfig startet mein Laptop nur mit 0x67

Sobald ich auf 0x0 oder 0x3 gehe bekomme ich das Verbotszeichen.

Im Terminal habe ich auch schon erfolglos den Befehl : sudo kextcache -invalidate / durchgeführt.

Unter Install Drivers sind bei installiert der:

OsxAptioFixDrv und der OsxAptioFixDrv2

Bei aktiviertem SIP und Verbose Start bekomme ich die Fehlermeldung:

OsxAptipFixDrv: Error - requested memory exceeds our allocated relocation block

Gruss

Beitrag von „griven“ vom 31. Juli 2017, 19:33

Das wird sich auch nicht ändern lassen bzw. ist ein wenig Maschinen abhängig. Die Meldung die Du bekommst sagt aus das nicht genügend Speicher verfügbar gemacht werden kann um den Prelinked Kernel mit aktivierter SIP zu dekomprimieren. OS-X entpackt nach dem Aufruf der boot.efi den Prelinked Kernel in den Systemspeicher wobei dafür ein zusammenhängender Speicherbereich in einem bestimmten Adressbereich vorhanden sein muss. Je nach System, Mainboard, Biosversion und verbauter Komponenten ist mehr oder weniger Speicher in diesem Adressraum bereits belegt bevor überhaupt das Betriebssystem gestartet wird (das passiert bereits durch das initialisieren der Hardware). Die Treiber OSXAptioFix bzw. OSXAptioFix2 sorgen durch das verschieben von Adressen in diesem Bereich dafür den Block von zusammenhängendem freien Speicher zu vergrößern was aber nur bedingt bis zu einem bestimmten Maß möglich ist. Je Mehr Features der SIP nun aktiviert werden sollen um so mehr Speicher ist nötig und um so wahrscheinlicher ist es das nicht genug Speicher freigeschaufelt werden kann.

Darf ich fragen warum es für Dich wichtig ist die SIP zu aktivieren? Ich denke jemand der es geschafft hat OS-X auf einem nicht dafür vorgesehenen Rechner zu installieren sollte doch eigentlich genug Ahnung von Computern haben um zu wissen das man nicht leichtfertig irgendwelche Dinge installiert und/oder irgendwelche Links in irgendwelchen Emails anklickt?

Beitrag von „Banduri1984“ vom 31. Juli 2017, 19:44

Danke Griven für die superschnelle Antwort.

Ich habe mir darüber keine Gedanken gemacht. Da ich in der Mac-Welt noch ein Grünschnabel bin,
habe ich das alles für wichtig empfunden.
Ich habe nicht gewusst dass das SIP eine Vorsichtsmassnahme für Idioten ist.
Und zur Not hat man ja auch noch Backups.

Das ist echt klasse. Du hast mir schonmal geholfen.
Und jetzt schon wieder.

Top top top.

Gruss

Beitrag von „griven“ vom 31. Juli 2017, 20:01

Naja die SIP hat auf Apples Computern schon ihren Sinn und ist einiges mehr als eine Vorsichtsmassnahme für Idioten aber eben auch nur da. Neben dem Dateisystem (was wirklich eher als Idioten Abwehr zu verstehen ist) wird unter anderem auch der Zugriff auf den NVRAM und andere Apple typische Dinge unterbunden. Ein MAC funktioniert eben doch immer noch ein wenig anders als ein PC und hier ist es schon möglich durch einen Zugriff auf das Dateisystem und den NVRAM ein potentiell kompromittiertes Firmware Image zu platzieren das der MAC dann beim nächsten Systemstart einfach installieren würde und zack ist die Laube infiziert. Das alles geht natürlich am PC so nicht denn hier laufen diese Prozesse anders und eher nicht ohne den Zugriff des Users ab zudem gewährt die auf PC´s notwendige Technik zum booten von OS-X (Clover, Enoch oder Ozmosis um mal nur die bekannten zu nennen) eine gewisse zusätzliche Sicherheit da durch sie noch mal eine Ebene zwischen Firmware und OS entsteht die auf einem Mac so nicht vorhanden ist.

Beitrag von „Doctor Plagiat“ vom 31. Juli 2017, 20:17

> Zitat von Banduri1984
>
> Unter Install Drivers sind bei installiert der:
> OsxAptioFixDrv und der OsxAptioFixDrv2

Falls du beide gleichzeitig benutzt ist das aber falsch. Immer nur einen verwenden.

Beitrag von „Altemirabelle“ vom 1. August 2017, 00:18

0x0 (SIP Enabled) kannst du nicht einstellen, da dein hackintosh mit dieser Einstellung nicht

funktionieren würde, aber 0x3 (SIP Partially Disabled - Loads unsigned kexts) ist möglich.
Versuche jedoch das zu machen was Doctor Plagiat gesagt hat. Immer nur einen OsxAptioFixDrv verwenden.

Beitrag von „griven“ vom 1. August 2017, 00:57

Abhängig von seinem System wird auch 0X3 nicht gehen denn jede Option die man mehr aktiviert bläst den Bedarf an Speicher weiter auf. Ich glaube nicht das er beide Fixes parallel installiert hatte (warum erlauben das die Installationsroutinen von Clover und/Oder CloverConfigurator überhaupt?) und selbst wenn würde er vermutlich in dem Fall auch mit 0x67 oder 0x7F nicht wirklich weiter kommen da sich beide gegenseitig aushebeln. Es ist schon schön das man auch am Hack die SIP wenigstens teilweise nutzen kann aber ob das nötig ist? Gut wenn ich plane den Computer jemanden in die Hände zu geben der so gar keine Ahnung von der Materie hat (User Level 0) mag das vielleicht Sinn machen aber selbst da eigentlich nicht wirklich einfach weil selbst mit komplett aktiver SIP unbedarfte User einen Hackintosh je nach unterliegender Hardware mit einem einzigen Klick ins Nirvana befördern können...

Beitrag von „Altemirabelle“ vom 1. August 2017, 08:57

Ich weiss natürlich nicht was das für ein Laptop ist, da in dem Thead die Beschreibung fehlt.
Ich kann dazu nur sagen, dass sogar für ein Laptop mit 4 GB RAM und OS10.11-12, SIP kein Problem ist.
Ob das nötig ist? Nein Griven. Aber in deiner Wohnung hast du auch ein Schloss an der Tür, und ich bin mir ziemlich sicher dass er auch benutzt wird. Jede Sicherheitsmaßnahme ist gut, und ich kann es einfach nicht glauben, dass Apple seine Kunden für Idioten hält und aus diesem Grund diesen Mechanismus einbaut und auch gleich aktiviert. Oder doch, hehehehehehe
In dem Fall will ich zu den Idioten gehören die das benutzen. 

Beitrag von „griven“ vom 1. August 2017, 10:08

Das hast Du falsch verstanden denn es kommt nicht auf die Menge des vorhandenen RAMS an.

Du kannst in so eine Kiste 16 oder 32GB stecken und den Fehler trotzdem bekommen. Es geht hierbei um zusammenhängenden freien Speicher in einem Adressbereich deutlich unterhalb der 2GB Grenze und der ist mal so gar nicht abhängig von der Gesamtmenge installiertem RAM. Das Stichwort an der Stelle ist die Memory Map (https://en.wikipedia.org/wiki/Memory_map). Was die SIP selbst angeht kann es natürlich nicht schaden sie zu aktivieren und damit den Zugriff auf das System für unbedarfte Nutzer einzuschränken allerdings macht das auf einem Hackintosh eben auch nur bedingt Sinn. Das hat nichts damit zu tun ob man ein Schloss an der Tür hat oder nicht. Wenn man Angst um die Daten auf seinem Laptop hat ist es tausendmal sinnvoller diese zum Beispiel mittels FileVault2 zu verschlüsseln als sich selbst den Zugriff auf das System durch die SIP einzuschränken aber gut jeder so wie er mag.

Beitrag von „Altemirabelle“ vom 1. August 2017, 16:06

Den Otto normalhackuser interessiert Memory Map überhaupt nicht und will eigentlich nichts davon wissen, sogar von SIP hat er selten gehört. Und nur weil es für die Installation wichtig ist. Er würde das so belassen, wie das die mächtige Firma Apple eingerichtet hat. Aber wenn es um Sicherheit geht, gibt es wenige die sagen, ja mach mal meinen Rechner etwas unsicher, ich bin immer aufmerksam und konzentriert. Ich bin sehr intelligent und klicke keine verdächtigen files an!
Um es klar zu sagen: SIP verhindert es nicht, dass man sich Malware einfängt. Allerdings verhindert die SIP, dass die Schadsoftware trotz der – durch die Passworteingabe eingeräumten – Admin-Rechte nicht noch das Betriebssystem manipulieren kann. So könnte die Malware dann beispielsweise den Dateisystem-Treiber so verändern, dass man die Dateien mit dem Schadcode nicht mehr entdecken kann. SIP begrenzt also allemal den Schaden.

FileVault ist sehr empfehlenswert, aber auch keine perfekte Sache. Das haben schon einige zu spüren bekommen, die 2 Partitionen auf einer HD haben.
Eine Firmware-Attacke per Firewire- und Thunderbolt-Schnittstelle ist auch möglich, da diese Schnittstellen per DMA den Arbeitsspeicher auslesen können.
Eine Schwäche von Filevault ist wohl vor allem der begrenzte Schutz gegen Brute-Force-Attacken. Es gibt bei Filevaut nämlich keinen Selbstzerstörungsmechanismus, man kann also unzählige Passwörter eingeben.

Wenn man Maximum an Sicherheit will, weil man etwas paranoid ist, sollte man vielleicht beides verwenden.

Ja aber wir streiten da und der Banduri1984 sagt nichts?

Beitrag von „griven“ vom 1. August 2017, 16:55

Ich würde das nicht streiten nennen wollen 

Man darf einfach diese Mechanismen nicht 1:1 von einem Mac auf einen PC übertragen denn beide Plattformen verhalten sich an der Stelle vielfach komplett unterschiedlich. Ein gutes Beispiel ist die Attacke auf die Firmware welche auf MACs durch die SIP erheblich erschwert wird aber auf einem PC schon als solches gar nicht greift weil eben das UEFI eines PC´s mit den Boardmitteln von OS-X gar nicht so ohne weiteres veränderbar ist. Eine Tatsache ist jedoch das einige Bestandteile der SIP den Betrieb eines Hackintosh erheblich erschweren und hiermit meine ich nicht mal nur die Restriktionen die durch das erzwingen von signierten Extensions entstehen.

Mir ist schon klar das Otto Normalhackuser in erster Linie User ist und mit solchen Dingen im Normalfall nichts zu tun haben möchte aber genau hier liegt auch eine erhebliche Gefahr denn das vielfach fehlende Verständnis der Dinge die da eigentlich passieren führt letztlich oft erst zu Fehlern und Problemen. Auch wenn sich ein Hackintosh weitestgehend so verhält wie ein Mac ist es eben trotzdem noch immer ein PC zusammengesetzt aus mainstream Hardware und der fehlen nun mal die Dinge die einen Mac zu einem Mac machen (SMC Device, AppleFirmware etc.). Die SIP ist ein gutes Beispiel für einen Mechanismus der darauf abzielt MacOS auf Mac Systemen zu härten und so zu verhindern das der User allzu unbedachte Dinge mit seiner Kiste anstellt und obendrein auch noch die Hardware vor Manipulationen schützt. Innerhalb dieses Ökosystems macht ein solcher Mechaninsmus Sinn denn der User soll keine Software installieren die nicht aus dem AppStore oder zumindest von einem verifizierten Entwickler stammt. Wohlgemerkt innerhalb dieses Ökosystems macht es Sinn der Haken ist nur mit einem Hackintosh bewegt man sich nicht innerhalb dieses Ökosystems Mechanismen wie die SIP werden auf unseren geliebten Hacks schon ausgehebelt bevor sie überhaupt greifen können. Die Möglichkeiten KernelExtensions in den KernelCache zu injecten oder innerhalb des Caches den Kernel oder Extensions beliebig zu patchen ganz und gar an allen gewollten Restriktionen vorbei zeigt wie wenig sinnvoll der Einsatz auf unseren Maschinen ist.

Du sagst ganz richtig Otto NormalHackUser will damit eigentlich nichts zu tun haben sollte sich allerdings troztdem lieber ein wenig mit den Hintergründen beschäftigen bevor er sich in eine Welt trügerischer Sicherheit flüchtet. Nur damit es nicht wieder falsch rüber kommt ich möchte mich nicht streiten und ich muss auch nicht unbedingt recht haben was ich möchte ist einfach nur ein wenig dafür sensibilisieren das solche Dinge auch mal hinterfragt werden und man wenigstens ein klein wenig aus dem Otto Normalusertum ausbricht. In diesem Sinne frei nach Steve Jobs - Stay Hungry, stay Foolish

---

Beitrag von „Banduri1984“ vom 1. August 2017, 19:00

Hallo Leute

Ich habe nun beide seperat getestet und das Ergebniss bleibt beim alten.
Besitzen tue ich ein Asus Ultrabook UX305FA.

Apple handelt natürlich auch aus einer anderen Position heraus. Ich kann für mich
Wissen aneignen und dieses anwenden. Apple hingegen muss immer
auch die breite Masse miteinbeziehen. Da gibt es ältere Menschen, Umsteiger,
Dumme, Intelligente was auch immer.
SIP gibt es auch erst seit El Capitan. Deswegen würde ich das auch nur um ein weiteres Sicherheitsfeature
deklarieren. So quasi als i Tüpfelchen.

Mein Werkzeugkasten beinhaltet einen wachen Geist, Backups und ein richtig
durchstrukturiertes Passwortmanagement. Das ist so ziemlich das schlimmste was dir passieren kann.
Wenn irgend jemand deine Passwörter hat.

Das beste System wird dir nichts nützen wenn du dich auf allen Seiten mit dem Passwort deines Geburtsdatum einloggst.