Erledigt Probleme nach Installation 10.13.3 mit NVIDIA Grafik

Beitrag von „griven“ vom 25. Februar 2018, 23:27

Nö muss eben nicht

Clover und auch OZ umgehen die SIP bevor sie überhaupt greifen kann was aber nur funktioniert wenn man alle nicht signierten Extensions von Clover oder eben OZ injecten lässt aber wie funktioniert das Ganze ?!? Apple packt einen sogenannten prelinkedkernel zusammen in dem sich neben dem Kernel selbst auch alle Extensions befinden die das System benötigt. Dieses KernelImage wird von der boot.efi beim Systemstart in den RAM entpackt und dann wenn das erledigt ist wird der Kernel gestartet und eben auch die SIP in Kraft gesetzt. Lässt man nun Clover oder OZ nicht signierte Extensions injecten passiert dies bevor der Kernel gestartet wird sprich vom Ablauf her sieht es so aus das sich Clover oder OZ zwischen das entpacken des Prelinked Kernels und den eigentlichen Start des kernels setzt. Die nicht signierten Extensions werden in den RAM platziert bevor der Kernel gestartet wird und et Voila wie haben unsere Extensions an der SIP vorbei ins System gebracht.

Aber warum funktioniert das? Ganz einfach weil Apple darauf vertraut das nichts in den prelinked Kernel kommen kann was da nicht sein darf. Auf echten Macs ist das auch so denn bei einem MAC gibt es erstmal keine Möglichkeiten etwas in den prelinked Kernel einzuschleusen solange die SIP aktiv ist und damit ist von der Warte Apples aus dem Sicherheitsanspruch genüge getan.
Was heißt das nun für uns? Für uns heißt das, das wir unsere Kisten getrost mit komplett aktiver SIP betreiben können solange wir uns daran halten unsere spezifischen Extensions in die EFI zu packen und nicht versuchen diese zum Beispiel mit dem KextUtility nach /S/L/E zu installieren denn das wird uns mit aktiver SIP nicht gelingen und somit erfüllt das Feature genau was es soll