Mod BIOS via Programmer flashen

Beitrag von „griven“ vom 18. September 2018, 21:59

Das Piepen kommt vom TPM und ist in sofern normal als das das TPM erkennt das ein modifiziertes Bios eingesetzt wird (die Checksumme bzw. Signatur ist nach der Modifikation ungültig). Man sollte sich vor dem aufspielen eines modifizieren Roms darüber im klaren sein das das TPM anschließend nicht mehr wirklich genutzt werden kann bzw. seinen Dienst mit den genannten Beeps quitiert weil die Plattform nun eben nicht mehr trusted ist. Sofern man unter Windows nicht gerade Bitlocker verwenden möchte kann man aber auf das TPM Feature relativ gut verzichten und das TPM im Bios einfach deaktivieren (SecurityChip -> Disabled) und schon ist Ruhe im Karton