BusKill-kabel schakelt laptop uit in geval van diefstal

Door **Security.nl** - 3 januari 2020

Schijfencryptie, sterke wachtwoorden en tweefactorauthenticatie moeten ongeautoriseerde toegang tot accounts en data voorkomen, maar doen weinig als iemand je laptop steelt terwijl je op allerlei accounts bent ingelogd. Aanleiding voor engineer Michael Altfield om "BusKill" te ontwikkelen.

BusKill is een script dat monitort of een usb-apparaat uit de laptop wordt verwijderd en vervolgens de computer uitschakelt. De laptopeigenaar zou een usb-stick direct in de laptop kunnen steken en die aan een kabeltje kunnen vastmaken. Het risico bij deze methode is dat de kabel kan breken en de usb-stick in de laptop blijft zitten. Een betere oplossing volgens Altfield is het dragen van de usb-stick op het eigen lichaam en die via een datakabel met de laptop verbinden.

Zodra een dief de laptop nu steelt vliegt de usb-stick uit de machine en wordt het script dat de machine uitschakelt actief. De dief heeft nu toegang meer tot de data. Ook wanneer de datakabel wordt doorgeknipt zal het script dit beschouwen als het uitwerpen van de usb-stick en de machine uitschakelen. Vooralsnog is

het BusKill-script alleen beschikbaar voor Linux.

Het risico dat een laptop wordt gestolen of in beslag genomen op het moment dat de gebruiker is ingelogd is niet theoretisch. Zo wachtte de FBI bij de aanhouding van de beheerder van de online marktplaats Silk Road totdat hij op zijn laptop was ingelogd. De kabel spreekt erg tot de verbeelding, zo blijkt uit de honderden reacties op Hacker News en Reddit.

Security.nl

http://www.security.nl