

Sicherheitsinformation!
Stinkende Grüße von LOJAX!

**Öffne zur eigenen Sicherheit keine E-Mails mit
@hgbecker.de oder marigott@..***

Der PC, den ich nun verschrotte, war mit Rootkits, LOJAX und Microsoft-Remote-Control gehackt und ausgespäht.

Was ist LOJAX ?

LOJAX ist ein Trojaner, der sich im BIOS festsetzt, vor dem Start von der Festplatte bereits im Hauptspeicher „Mist schaufelt“ und vorhandene und fabrikneu eingebaute Festplatten und angesteckte USB-Sticks und externe Festplatten unrettbar verseucht.

Wer den Schaden hat und danach liest, dass die BIOS-BOOT-Option **SECURE BOOT** → **ENABLED** dagegen schützt, stellt fest, dass sich eben diese und ein BIOS-Passwort nicht mehr einstellen lassen.

Durch Sichten und Testen dieser BIOS-Einstellungen lässt sich LOJAX so schnell feststellen. Dann ist es ratsam, den PC gar nicht mehr starten zu lassen (Starttaste zum Ausschalten halten), um Weiterverteilung des Trojaners und erpresserische Verschlüsselung der Festplatten zu behindern.

Aber wer von uns weiß das schon vorher?

Microsoft hat mit Rootkits (unsichtbare Dateianhänge, deren Vorhandensein und Größe nicht angezeigt werden), mit zuerst als Diebstahlsicherung propagierter und versteckter Herstellerangabe auf Festplatte, die bei Neuinstallation nicht überschrieben wird und Remote Control (Rechnerfernsteuerung) selbst die Wege für Betrügereien und Ausspähen geebnet. NSA und Osteuropäische Hacker sind mit von der Partie.

Einfachster Weg, sich diesen Unrat zu holen, ist Öffnen von Links und Anhängen von E-Mails. Da auch E-Mail-Adressen ausgespäht wurden, können gefälschte E-Mails, angeblich von meiner Sendeadresse, oder von anderen Adressen bei Dir eingehen. Öffne in diesen keine Links oder Anhänge, frage ggf. telefonisch den Dir bekannten Absender, ob die Nachricht von ihm ist. Lösche Mails der oben in rot genannten Absender sofort und von unbekanntem Absendern sofort, egal ob im Eingangs- oder im Spamordner.

Vielfach versandte Phishing-Mails zur Eingabe von Kontodaten sind leicht durchschaubarer Kleinkram gegen die Gefährlichkeit und die Bitcoin-Fraßkrankheit der Lojax-Erpresser-Clique.