Teil 4: Daten verschlüsseln - einfach erklärt!

Auch dieses Video ist gut gemacht, bezogen auf die Empfehlung von TrueCrypt aber leider aus der Zeit gefallen. Wie erwähnt, wird diese Software seit 2014 nicht mehr weiter entwickel. Was der Film allerdings beschreibt lässt sich mittlerweile 1:1 auch auf **VeraCrypt** übertragen, einschließlich der Verifikation des Quellcodes. Auch hier gab es mindestens ein erfolgreich bestandenes *Bug Bounty*. Die Software enthält keine erkennbaren, die Sicherheit gefährdenden Fehler. Die Installation und auch die Bedienung laufen ab wie gezeigt (einschließlich der Bewegung der Maus).

Was mir noch wichtig wäre: Laufwerke mit Daten verschlüsseln – ja, doch niemals das ganze Systemlaufwerk. Das ginge zwar, wäre aber nach meiner Einschätzung gefährlich. Ich persönlich ziehe verschlüsselte Datencontainer vor. Die lassen sich leichter an verschiedene Orte verteilen, wie im Video beschrieben. Ganze Festplatten können bei der Übertragung der Inhalte sehr viel Zeit beanspruchen. Wir reden hier über Backups essentieller oder uns wichtigen Daten. Ich zitiere auch hier das Video: „Daten existieren nur dann, wenn sie an mindestens drei verschiedenen Orten gespeichert sind“. Wenn die Daten vorher (!) verschlüsselt wurden, ist auch die Cloud ein sicherer Ort.

Eine weitere Option der Software, das „Verstecken der Daten“ ist für wirkliche Spezialisten keine Sicherheit vor Entdeckung. Über statistische Methoden lässt sich im Rauschen einer scheinbar formatierten Platte durchaus der Nachweis existierender Inhalte erbringen. Es wäre zwar immer noch nicht lesbar aber eventuell reden ja der Besitzer oder die Besitzerin?