Die Kryptokalypse in allernächster Zukunft?

Erfasst am : 5. September 2022 13:15 | Erfasst von : Martin
Verknüpfte Kategorie(n): Internet, Diverses, Kommerz

Ich bin ja ziemlich versiert in Kryptografie. Daher empfand ich den Text auf Heise sehr eindringlich und möchte hier diesen verbreiten.

Auch wenn die wenigsten sich mit Kryptografie beschäftigen, will wohl jeder sicher sein, dass eine angesurfte Website die ist, die man meint. Oder dass Datenverkehr übers Internet, die Online-Zahlung zumindest auf dem Weg von mir zum Ziel unknackbar ist. Dass ein Testament, ein Vertrag, eine Beglaubigung nicht fälschbar ist.

Der Quantencomputer (QC) ist das Damoklesschwert, das über der modernen digitalen Kommunikation hängt. Kann ein QC elliptische Kurven oder RSA knacken, ist **ALLES BISHERIGE GESPEICHERTE** ein offenes Buch für alle Interessierten - seien es White oder Black Hat Hackers. Und da sich wohl nur Staaten oder Reiche einen QC leisten können, heisst das wohl, dass wiedermal nur die oberen 10000 (oder weniger) davon profitieren. Und wir anderen stehen in der digitalen Kommunikation mit heruntergelassenen Hosen / Röcken da.

In aller Klarheit: Alles bisherig Signierte oder Verschlüsselte ist dann lesbar! Da Datenkraken ja mindestens seit 15 Jahren alles speichern, ob es nun heute knackbar ist oder nicht, heisst das, dass **RÜCKWIRKEND** alles lesbar wird. Das kann sogar lebensgefährlich werden für Leute, die das TOR-Netzwerk benutzen, um aus gefährlichen Umgebungen digital zu kommunizieren.

Die Forschung ist daher angehalten, Algorithmen zu entwickeln, die (selbstverständlich) jedem Angriff von konventionellen Supercomputern aber auch eben dem QC widerstehen können.

Dieser Artikel Kryptokalypse transportiert diese Botschaft so, dass wir in der digitalen sicheren Kommunikation noch etwa 4 Jahre vor dem Abgrund, der totalen Vernichtung aller bisherigen digitalen Vertrauenssicherheit stehen. Das Tragische an der Geschichte ist, dass mit Verschlüsselung geschüttze Leute wie Dissidenten oder andere staatlich Verfolgte dann ja noch leben. Nicht auszudenken, was Diktaturen wie Russland etc. dann mit diesen Leuten machen ...

Ohne einen neuen Algorithmus würden alle elektronischen Daten vor einem QC nicht mehr sicher sein. Privacy adé. Das in den Datenhalden der Grossen Player gespeicherte Zeug ist sowieso schon Makulatur, denn ein QC wird wohl elliptische Kurven und RSA knacken können in wenigen Jahren. Also, die digitale Apokalypse ist sowieso unausweichlich.