Duo schlägt gegen Wanna Cry zurück

Uffenheimer Firma kann nach Virus-Angriff Daten retten – Milliarden-Schaden im Mai

UFFENHEIM – Computer-Experten weltweit zucken beim Begriff „Wanna Cry“ zusammen. Es handelt sich um einen Virus, der Mitte Mai für einen der größten Hacker-Angriffe der Geschichte genutzt wurde. Der betriebswirtschaftliche Schaden wird auf mehrere Milliarden Dollar geschätzt. 200 000 Firmen und Institutionen waren betroffen. Ein Zwei-Mann-Unternehmen aus Uffenheim glaubt, im Notfall Hilfe leisten zu können.

Findet der Wanna-Cry-Virus einen Weg auf einen Rechner, verschlüsselt er die Dateien darauf und legt den Code dafür im Arbeitsspeicher ab. Dann erscheint eine Meldung am Bildschirm, dass der Computer übernommen wurde und nur durch die Zahlung einer bestimmten Geldsumme in der Internet-Währung Bitcoins wieder freigegeben werde.

Reflexartig schalten viele Nutzer ihren Computer aus – und zerstören somit die Daten, wie Jannik Herrmann von der Uffenheimer Firma Itka Systemhaus erklärt. Der Arbeitsspeicher wird durch das Abschalten des Stroms gelöscht, der Code zum Entschlüsseln vernichtet. Um zumindest einen Teil der Daten auf den Festplatten zu retten, durfte – so die gängige Lehrmeinung in der Szene – der Rechner nur vom Internet, aber nicht vom Stromnetz gekappt werden.

Nach der Attacke im Mai sei dann ein verzweifelter Chef einer Firma mit 15 Mitarbeitern bei Itka, die sich auf IT-Sicherheit spezialisiert haben, aufgeschlagen und bat um Hilfe. Man habe ihm gesagt, die Daten auf seinen Firmenservern seien für immer verloren. Auch er hatte alles abgeschaltet. „Also hat mein Kollege ein Programm geschrieben und mit der Software hat es funktioniert“, sagt Herrmann, der aus Bad Windsheim stammt.

Schwäche in der Logik

Der Virus hat offenbar Schwächen. Eine führt unter anderem dazu, dass die Überweisung der erpressten Bitcoins normalerweise nicht funktioniert, weil die Angreifer das Geld nicht einem bestimmten Code zuweisen können. Der Rechner bleibt also gesperrt. Das könne man sich also gleich sparen, rät Herrmann, der den genauen Ansatzpunkt der Rettungs-Software aber nicht verraten will. Nur: „Es ist ein Fehler in der Logik des Virus, den wir ausnutzen.“

Jannik Herrmann und sein Kollege Philipp Kahler trauen sich – obwohl sie ihr Programm erst einmal testen konnten – sagen, dass sie nach einem Angriff mit Wanna Cry „mit hoher Wahrscheinlichkeit“ alle Daten wiederherstellen können. Je nach Größe der Festplatten nehme die Rettung ein bis zwei Wochen pro Server in Anspruch.

Aus der Wirtschaft

Der Angriff vom Mai liegt zwar schon ein wenig zurück, doch Wanna Cry und ähnliche Viren sind stets im Umlauf und suchen sich selbstständig neue Ziele über Netzwerke. Vor allem kleinere Firmen und Privatleute seien anfällig für Datenverluste, weil ihnen meist die Backups fehlen. Herrmann: „Das darf man nicht vernachlässigen. Wenn alle Daten weg sind, könnte eine Firma den Bach runtergehen.“

BASTIAN LAUER

Philipp Kahler (links) hat ein Programm zur Rettung nach Angriffen mit dem Wanna-Cry-Virus geschrieben. Jannik Herrmann ist auch begeistert. Foto: Privat