BitcoinBlog.de
Das Blog für virtuelle Währungen

Hacker infiltrieren Krankenhaus und verlangen 9.000 Bitcoin Lösegeld

Posted on 15. February 2016 by Christoph Bergmann // 3 Comments

ambulance von Till Krech via flickr.com. Lizenz: Creative Commons

Das Hollywood Presbyterian Medical Center in der Mitte von Los Angeles hat ein Problem. Hackern ist es gelungen, das Computersystem des 430-Bett-Krankenhauses außer Betrieb zu setzen. Für die Herausgabe der Schlüssel, die das System wieder aktivieren, verlangen die Cyberkriminellen 9.000 Bitcon, was derzeit rund 3,2 Millionen Euro entspricht.

Das 21. Jahrhundert wird vielleicht als Zeitalter der Kryptoanarchie in die Geschichte eingehen: als eine Zeit, in der IT-Systeme mehr und mehr lebensnotwendige Funktionen ausüben, aber zugleich zu Einfallstoren für Kriminelle aus dem Cyberspace werden. Einen Vorgeschmack, wie das ausgehen kann, erhielten Patienten des Hollywood Presbyterian Medical Centers. Sei einigen Wochen werden Untersuchungsergebnisse per Faxt anstatt per E-Mail verschickt, Aufnahmen mit Stift und Papier anstatt mit Computern dokumentiert und Patienten wegen alltäglicher Behandlungen an andere Kliniken weitergeleitet.

Das Krankenhaus mit seinen 430 Betten fiel einem schweren IT-Angriff zum Opfer. Wie es aussieht, hat ein Virus, der irgendwie ins System eingedrungen ist, die Datenbanken verschlüsselt. Die Folge: Ärzte können nicht mehr zeitnah auf Patientendaten zugreifen, der Datentausch mit Laboren, Röntgengeräten und Computertomographen ist unterbrochen und Strahlungsgeräte sowie die Onkologie sind ausgeschaltet. Softpedia berichtet, dass mehr als 900 Patienten in andere Krankenhäuser geschickt wurden.

Der Hack ereignete sich Anfang Februar, wurde aber erst heute publik und ist noch nicht gelöst. Die lokale Polizei, das FBI sowie eine Firma für Computer-Forensik ermitteln, jedoch bislang wohl noch ohne Ergebnisse.

Die Hacker fordern 9.000 Bitcoins für die Schlüssel für das System, was im Moment, bei einem Kurs von 360,07 Euro, ansehnlichen 3.240.630 Euro entspricht.

Ob die Klinik zahlt oder nicht, ist ebensowenig bekannt wie technische Details über den Hack. Softpedia spekuliert über zwei Szenarien: In beiden hat eine Inkarnation der gewöhnlichen Ransomware das System infiltriert. Ransomware gelangt zum Beispiel durch eine E-Mail von angeblich einer Bank auf Computer, verschlüsselt dort alle Festplatten – auch USB-Sticks! – und verlangt 0,5-1 Bitcoin für den Schlüssel. Im ersten Szenario hat der Virus so viele Computer infiziert, dass das Lösegeld für das ganze System der Klinik 9000 Bitcoin erreicht. Oder – und das finde ich viel wahrscheinlicher: Die Hacker haben die Lösegeldforderung "etwas" erhöht, nachdem ihnen klar wurde, was für ein Fisch ihnen ins Netz gegangen ist.

Ransomware ist eine Plage des Internets. Die Welt wäre ohne sie bestimmt besser, wie ohne Schnaken, aber sie wird daran auch nicht kaputtgehen. Ich glaube, Cyber-Mobbing ist schlimmer. Je mehr sich aber Wirtschaft und Gesellschaft und alles mit dem Internet verbinden, Autos, Fabriken, Behörden, Herzschrittmacher, Geld und eben Krankenhäuser, desto größer wird die Bedrohung durch Mal- und Ransomware. Der Fall des Hollywood Presbyterian Medical Center ist der bisher größte bekannte Hack für Bitcoins, dürfte aber erst der Anfang sein.

Eine Fußnote: vor einigen Tagen wurde auch die Webseite der britischen Vereinigung der Berater und Psychotherapeuten von Ransomware angegriffen. Sie ist derzeit offline. Anders als beim Hollywood Krankenhaus begnügen sich die Hacker jedoch mit 0,4 Bitcoin. Beunruhigend ist allerdings, dass die Webseite auf einem Linux-System läuft, von dem man bisher sagt, es sei weitgehend virensicher. Anscheinend wurde der Virus speziell dazu geschrieben, Webseiten lahmzulegen.

Ein verheerendes Detail von Ransomware im Allgemeinen ist, dass ein Angreifer mit relativ geringem Aufwand einen hohen Schaden anrichten kann. Er muss nicht mal programmieren können. Erst vor einem Monat fanden Sicherheitsforscher heraus, dass im DeepWeb bereits Ransomware-as-a-service angeboten wird. So kann jeder zum digitalen Erpresser werden.