Süddeutsche.de Wirtschaft

25. März 2019, 18:51 Computerfirma Asus

Opfer eines Hacker-Angriffs

Von Max Muth

Der taiwanesische Computerhersteller Asus ist offenbar Ziel eines komplexen Hacker-Angriffs geworden. Einem Bericht der IT-Sicherheitsfirma Kaspersky zufolge haben es die Angreifer geschafft, einen offiziellen Update-Server der Firma zu kapern, sodass die attackierten Computer dachten, sie würden ein gewöhnliches Update für Asus-Geräte herunterladen. Stattdessen luden sie Malware auf ihre Rechner. Zuerst über den Fall berichtet hatte die US-Journalistin Kim Zetter für das US-Tech-Portal Motherboard. Demnach lief die von Kaspersky Lab "ShadowHammer" getaufte Attacke zwischen Juni und November 2018. Entdeckt wurde sie im Januar 2019. Dem Unternehmen zufolge waren 57 000 Kaspersky-Kunden betroffen, die IT-Sicherheitsfirma Symantec gab die Zahl ihrer betroffenen Kunden mit 13 000 an. Kaspersky schätzt, dass insgesamt mehr als eine Million Nutzer betroffen gewesen sein könnten.

Sollte die Analyse von Kaspersky sich bestätigen, wäre der Angriff aus mehreren Gründen bemerkenswert: Zum einen haben es die Angreifer offenbar geschafft, ein Update mit Schadcode auf dem offiziellen Update Server einer großen Computerfirma zu installieren. Das Update war demnach zudem noch mit einem vertrauenswürdigen Zertifikat von Asus signiert. Ein weiteres ungewöhnliches Detail: Zwar wurden wohl mehrere Hunderttausend Rechner infiziert, eigentliches Ziel der Attacke waren laut Kaspersky jedoch nur einige wenige Hundert Geräte, deren MAC-Adresse (eine Art Geräte-ID) in dem Schadcode hinterlegt war. Wenn das Schadprogramm auf einem der gesuchten Geräte landete, dann lud das schädliche Update automatisch weitere Malware von einem Server nach, den die Hacker kontrollierten.

Sogenannte Lieferketten-Attacken auf die Cybersicherheit von Produkten und Services nehmen zu. Dabei wird Schadcode schon bei der Produktion von Hardware oder Software eingebaut und muss nur noch aus der Ferne aktiviert werden. Wer hinter dem Angriff bei Asus steckt, ist nicht ganz klar. Der Chef der Forschungsabteilung von Kaspersky, Costin Raiu, weist allerdings auf Parallelen zu einer weiteren Lieferketten-Attacke hin: Die "ShadowPad"-Attacke versteckte 2017 bösartige Software in einem von der Finanzindustrie genutzten Service. In einem späteren Gerichtsprozess legte sich Microsoft fest, die Attacke sei von der Hackergruppe "Barium" ausgeführt worden. Die wiederum wird China zugeordnet.