SOPHOS

Security made (very) simple:

FBI-Direktor sichert seine Webcam mit einem Klebestreifen. Warum Sie seinem Beispiel folgen sollten.

Autor: Chester Wisniewski, Sicherheitsexperte bei Sophos

FBI-Direktor James Comey hielt vor einigen Wochen eine Rede am Kenyon College in Ohio. Der Inhalt: Die absolute Privatsphäre gibt es nicht und es hat sie, zumindest in Amerika, auch noch nie gegeben. Bis jetzt, wo standardisierte Verschlüsselungslösungen Räume schaffen, in die Strafverfolgungsbehörden den Verdächtigen nicht folgen können – noch nicht einmal mit einem gültigen Gerichtsbeschluss.

Comey kritisiert in seinen Reden immer wieder, dass die Verschlüsselung von Produkten des täglichen Bedarfs die Privatsphäre viel mehr berücksichtige, als die allgemeine Sicherheit. Während einer Frage-und-Antwort-Sitzung mit Schülern im Anschluss an eine solche Rede in Ohio gestand Comey, er hätte ein Stück Tape über die Webcam seines persönlichen Laptops geklebt – zur Sicherheit.

Die Idee ist gut und einfach. Spione und Hacker haben ein besonderes Interesse an privaten Profilen und Daten von Regierungsbeamten. Über eine untergeschobene Schadsoftware wie beispielsweise einen Remote-Access-Trojaner (RAT), kann der Computer übernommen, die Gespräche aufgezeichnet und die Webcam eingeschaltet werden. RATs eignen sich hervorragend zur Überwachung – das weiß auch das FBI. Gerichtsakten belegen, dass die Behörde selbst eine sehr ähnliche Malware verwendet, um Computer von Verdächtigen zu infizieren.

Das Tape erwähnte Comey im Rahmen seiner Antwort auf die Frage eines Studenten über Panoptismus, also allgegenwärtige Überwachung und welche Auswirkungen es hat, wenn die Menschen sich diese bewusst machen. Snowdens Veröffentlichungen bezeichnete Comey als "gute Sache". Sie ließen die Menschen erkennen, dass sie selbst eine Entscheidung zu treffen hätten darüber, wie die Regierung Sicherheit und Privatsphäre gewichtet: „Ich glaube nicht, dass es Grund zur Nervosität gibt. Sie sollten Kenntnis über die Details verlangen. Sie sollten wissen, wie die Behörden Überwachungen durchführen und wie sie selbst überwacht werden. Sie sollten wissen, wie die betreffenden Geräte funktionieren und was letztendlich die Wahrheit ist. Ich habe mir das Zukleben der Webcam von jemandem abgeschaut, der klüger ist als ich. Besonders junge Leute sollen ein gesundes Bewusstsein für dieses Thema entwickeln, sollten alle Informationen verlangen und sich engagieren.“

Was Sie gegen RATs tun können

Einer der bekanntesten Fälle, in denen RATs zum Einsatz kamen, war der von der Miss Teen USA Cassidy Wolf, die von Kriminellen erpresst wurde. Diese hatten sich

über einen RAT, bekannt als „Blackshades“ Zugriff auf ihren Computer verschafft und dann per Webcam Nacktbilder von ihr aufgenommen.

Der Trojaner kann jedoch weit mehr als nur Bilder machen. Mit seiner Hilfe können Kriminelle Passwörter und Bankdaten stehlen, sich in Social-Media-Konten hacken, Zugriff auf Dokumente, Fotos und andere Computerdateien erhalten, Tastenanschläge aufzeichnen, den Computer für Distributed-Denial-of-Service (DDoS)-Attacken missbrauchen oder den gesamten Inhalt verschlüsseln und den Besitzer erpressen.

Folgendes können Sie zum Schutz gegen Trojaner-Angriffe unternehmen:

- Decken Sie Ihre Webcam ab, wenn Sie diese nicht verwenden. Nehmen Sie blickdichtes Klebeband, oder drehen Sie die Kamera gegen die Wand. Ist sie integriert, schließen sie das Cover. Ist keines vorhanden, können Sie hier eines bestellen: The Sophos Store.
- Patchen Sie Ihr Betriebssystem (Windows, OS X) und alle Anwendungen (Web-Browser, E-Mail- und Messaging-Client, etc.), sobald Sicherheitsupdates verfügbar sind.
- Malware wird zumeist per E-Mail verbreitet. Seien Sie also vorsichtig mit Links und Anhängen in E-Mails oder Social Media Nachrichten von Fremden. Auch Meldungen, die von Bekannten und Freunden, könnten durch Hacker gefälscht werden.
- Installieren Sie Sicherheitssoftware um auf dem neuesten Sicherheitslevel zu bleiben.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de