



Wenn der Bordcomputer Deines Autos oder des Flugzeugs, in dem Du sitzt von der CIA oder vom MI5 gehackt wird, können diese Geheimdienste einen tödlichen Unfall herbeiführen und niemand könnte das beweisen. (Bild: Symbolbild, Fotomontage Niki Vogt, Bildquelle: Pixabay)

Wikileaks: MI5 und CIA kontrollieren Fernsehgeräte und Smartphones und könnten über Auto-Bordcomputer tödliche Unfälle herbeiführen

25. April 2019 | <https://connectiv.events/wikileaks-mi5-und-cia-kontrollieren-fernsehgeraete-und-smartphones/>

Unsere lieben smarten Helferlein im Alltag haben eine dunkle Seite. Sie sind gewissenlos und liefern ihre Besitzer dunklen Mächten aus. Sie verraten uns, wo wir gehen und stehen an Lauscher und Spione.

Und noch mehr: möglicherweise töten sie uns sogar auf geheimdienstlichen Befehl.

WikiLeaks deckte jedenfalls auf, dass der Britische Geheimdienst zusammen mit der CIA Fernseher und Smartphones in Abhörgeräte verwandelt, um Gespräche aufzuzeichnen. [Durchgesickerten Geheimdienst-Dokumenten zufolge](#) können sie uns damit sogar unbemerkt fotografieren.

Der CIA wirft WikiLeaks damit vor, ein geheimes Computer-Hacking-Programm laufen zu lassen, das ihren Agenten Zugriff auf allerlei smarte Alltagsgegenstände wie Mobiltelefone, Fernseher und iPads, Laptops usw. gewährt.

Besonders alarmierend: Ein anderes Dokument legt nahe, dass dieses – von der Cyber-Direktion der CIA entwickelte – MI5-CIA Spionageprojekt sogar auch auf Autos, LKWs und andere Transportmittel, wie Flugzeuge Zugriff haben soll, einfach alles, was einen Bordcomputer installiert hat, der mit dem Internet verbunden ist. Angeblich sollen die Geheimdienste, sobald sie die Kontrolle über Fahrzeuge erlangt haben, auf diese Weise Ermordungen inszenieren können und es wie Unfälle aussehen lassen. „Der Zweck einer solchen Kontrolle ist in den Dokumenten nicht genannt, aber es würde der CIA erlauben, so gut wie unaufdeckbare Tötungen durchzuführen“, sagte WikiLeaks.

Insgesamt veröffentlichte WikiLeaks dieses erschreckende Material im Rahmen von 8.761 Dokumenten. Laut WikiLeaks sei das seine bisher größte Veröffentlichung von CIA-Dateien.

Die CIA lehnte eine Stellungnahme ab. Datenexperten zeigen sich überzeugt, dass die zwischen 2013 und 2016 von der „*Engineering Development Group*“ der CIA erstellten und später durchgestochenen Dokumente echt seien.

Die britischen Geheimdienste – MI5 und GCHQ – sind laut dieser geleakten Daten in die Machenschaften der CIA tief verwickelt, denn die Dokumente zeigen klar, dass Großbritanniens Geheimdienste zusammen mit der CIA Workshops durchführten, wie man sich in Haushaltsgeräte „einhacken“ kann. Dieses Programm unter dem befremdlichen Namen „Weeping Angel“ (weinender Engel) ermöglichte es den Diensten konkret, in die Samsung TV-Geräteserie F8000, die serienmäßig immer mit dem Internet verbunden ist, hineinzukommen und das Gerät zu kontrollieren. Dieser „Hack“ wurde in einem „gemeinsamen Workshop“ entwickelt, der im Juni 2014 zwischen MI5 und der CIA stattfand, und ermöglichte es den Agenturen, diese Fernsehgeräte komplett unter Kontrolle zu bekommen.

Damit der Apparat nicht durch Ausschalten für die Spionagezwecke unbrauchbar wird, soll der MI5 einen sogenannten ‚Fake-Off‘-Modus geschaffen haben. Das bedeutet, dass der Fernsehbenutzer den Apparat zwar ausschaltet, der sich aber nur scheinbar ausschaltet und nur im Off-Modus zu sein scheint, in Wirklichkeit aber heimlich weiter läuft. Das Gerät kann so alles weiter aufzeichnen, während der ahnungslose Besitzer den Fernseher für ausgeschaltet hält. Alles, was das Gerät aufzeichnet, wird über Internet direkt an einen CIA-Mitarbeiter weitergeleitet, der sozusagen live mithören kann. Das funktioniert bestens dadurch, dass diese Fernseher über ein eingebautes Mikrofon verfügen, um eine sprachgesteuerte Bedienung zu ermöglichen.

Die an WikiLeaks gelangten Dokumente sollen auch aufzeigen, dass [GCHQ](#) mit der CIA zusammengearbeitet hat, um Apple-iPhones hacken zu können sowie auch alle anderen Smartphones, die mit Googles Konkurrenz, der Android-Software, als Betriebssystem arbeiten.

Diese Telefone können ihre Umgebung sogar dann aushorchen und fotografieren, wenn die Besitzer sie für ausgeschaltet halten. Laut den Dokumenten von WikiLeaks arbeitete dieser Kryptographie-Geheimdienst GCHQ, die im britischen Cheltenham ansässige Abhöragentur der Regierung, bereits 2017 intensiv an sechs verschiedenen Methoden, wie man in das Apple-iOS-Betriebssystem eindringen, das auf iPhones, iPods und iPads verwendet wird, sowie an Methoden zum Ausspionieren von Android-Handys. Insgesamt soll – den Dokumenten zufolge – die CIA vierzehn Wege zum „Einhacken“ auf iPhones und 24 zum „Einhacken“ auf Android-Smartphones und Tablets entwickelt haben.

Wikileaks behauptete weiterhin, dass auch Messenger-Apps nicht sicher seien. Die CIA sei durchaus in der Lage, die Verschlüsselungscodes zu umgehen, die als Sicherheit in Gruppen wie WhatsApp verwendet werden. Dazu soll die CIA angeblich Schwachstellen in der Technologie ausgenutzt haben, die nicht einmal den Geräte-Herstellern oder Designern bekannt sind – in der Geheimdienstwelt „Zero Days“ genannt -, um sich in die Geräte zu hacken.

Aus den Dokumenten geht hervor, dass die Agentur mehr als 1.000 Viren und andere Arten von Malware erstellt hat, um Zugriff auf Alltagsgegenstände zu erhalten.

WikiLeaks warf der US-Regierung außerdem vor, dass sie ihrer Verpflichtung nicht nachgekommen sei, Technologieunternehmen über festgestellte Schwachstellen zu informieren. Stattdessen würde sie die gefundenen Schwachstellen „horten“, damit die Geheimdienste sie nutzen können. Die Vereinbarung, Technologiefirmen über die „Hintertürchen“, die in ihren Geräten existieren, zu informieren, wurde gerade zu dem Zweck getroffen, dass die Technologie-Riesen diese Schwachstellen in ihren Betriebssystemen beseitigen und dadurch Lecks für ausländische Geheimdienste, insbesondere Russland und China, zu schließen.

WikiLeaks behauptete, das durchgestochene Dokumenten-Archiv sei zuvor von der CIA an ehemalige amerikanische Regierungshacker und -unternehmer verteilt worden. Einer der Empfänger habe WikiLeaks einen Teil des Cache-Speichers übergeben, um eine öffentliche Debatte über diese staatlichen Geheimdienstmethoden zu auszulösen.