

[Artikel drucken](#)[Als E-Mail versenden](#)[Artikel schliessen](#)[zur Seite](#)

122889957

Von Christoph Dernbach, dpa

Berlin. Der Skandal um die Abhöraktivitäten der NSA und ihres britischen Pendant GCHQ nimmt immer größere Dimensionen an. Wie jetzt bekannt wurde, hat der US-Geheimdienst mit Hilfe der Briten schon vor Jahren den weltgrößten Hersteller von SIM-Karten und anderen Sicherheitschips, das niederländische Unternehmen Gemalto attackiert. Seitdem können die Dienste offenbar die geheimen Schlüssel vieler Smartcards und SIM-Karten mitlesen. Dies geht aus Dokumenten des Whistleblowers Edward Snowden hervor, die am Donnerstagabend vom Investigativ-Portal "The Intercept" veröffentlicht wurden.

Die Attacke greift das Fundament der mobilen Kommunikation an: "SIM-Karten sind der Vertrauensanker aller Sicherheitsvorkehrungen in Mobilfunknetzen", sagte Linus Neumann vom Chaos Computer Club (CCC). "Wer im Besitz der auf den SIM-Karten gespeicherten Krypto-Schlüssel ist, kann alle Telefonate der betroffenen SIM-Karten abhören. Das betrifft sowohl zukünftige und auch in der Vergangenheit aufgezeichnete Gespräche." Wenn sich die Schlüssel in den Händen der Geheimdienste befinden, seien alle eingebauten Sicherheitsmaßnahmen, die ein Abhören von Telefonaten verhindern sollen, obsolet.

Spätestens seit dem Angriff der anglo-amerikanischen Dienste auf das Handy von Bundeskanzlerin Angela Merkel (CDU) hat sich herumgesprochen, dass man dem Mobilfunknetz in Sachen Abhörsicherheit nicht vertrauen kann. Der SIM-Hack eröffnet den Geheimdiensten nun aber ganz neue Möglichkeiten. So können NSA und GCHQ nun auch Gespräche und Datenverbindungen abhören, die über modernste Mobilfunktechnologien wie UMTS oder LTE geführt werden. Diese galten bislang als sicher beziehungsweise nur mit größerem Aufwand knackbar.

Wenn NSA und GCHQ die Schlüssel der SIM-Karten bereits besitzen, sind sie auch nicht mehr auf die Mithilfe der Justiz und der Mobilfunkprovider bei Abhörmaßnahmen angewiesen. Nach Einschätzung des CCC können die Dienste außerdem nicht mehr nur vor Ort aktiv werden, sondern auch weltweit abhören, ohne dabei entdeckt zu werden. Die Dienste können nach Einschätzungen von Experten den Klau auch dazu verwenden, die Endgerätekennungen (IMEI) der Handys auszuspähen. Ein Geheimdienst könnte damit ein Ziel auch weiter verfolgen, wenn die SIM-Karte ausgetauscht wird.

Während die Koalitionsparteien am Freitag die neuen Dimensionen des NSA-Skandals unkommentiert ließen, kritisierten Grüne und die Piratenpartei das Vorgehen der Geheimdienste scharf. "Für die IT-Sicherheit und die Integrität von IT-Infrastrukturen gibt es derzeit keine größer Gefahr als die Geheimdienste befreundeter Staaten, die sich rechtsstaatlich offenbar nicht mehr gebunden fühlen", erklärte der Grünen-Obmann im NSA-Untersuchungsausschuss, Konstantin von Notz. "Nicht Hackerbanden, sondern sie sind gegenwärtig das zentrale Problem für die IT-Sicherheit."

Die Krypto-Schlüssel auf den SIM-Karten wurden offenbar geklaut. dpa

[Artikel drucken](#)[Als E-Mail versenden](#)[Artikel schliessen](#)[zur Seite](#)