SPIEGEL ONLINE
13. April 2015, 15:40 Uhr

**Datenverschlüsselung**

# NSA-Chef will Krypto-Schlüssel teilen

**"Vordereingang" statt Hintertür: Michael Rogers hat einen neuen Vorschlag zum Umgang mit verschlüsselten Daten gemacht. Der NSA-Chef will Krypto-Schlüssel aufteilen.**

NSA-Chef Michael Rogers meint eine Lösung für ein Problem gefunden zu haben, das Anwender, Unternehmen und Behörden gleichermaßen beschäftigt: die Datenverschlüsselung. Spätestens seit Apple und Google ihre Mobil-Betriebssysteme so umgebaut haben, dass nicht einmal sie selbst Zugriff auf darauf gespeicherte verschlüsselte Daten haben, ist die Ermittlungsarbeit für Geheimdienste und Strafverfolgungsbehörden erheblich schwieriger geworden.

Laut "Washington Post" hat Michael Rogers nun vorgeschlagen, dass derart verschlüsselte Daten über einen Schlüssel gesichert werden sollen, der aus mehreren Teilen besteht. Diese Teile sollen an verschiedene Institutionen verteilt werden, also beispielsweise den Hersteller eines Handys und das FBI. Nur wenn alle Beteiligten in einem Einzelfall einverstanden sind, könnten die Einzelteile wieder zu einem funktionierenden Schlüssel zusammengefügt und die damit codierten Daten gelesen werden.

"Ich will keine Hintertür", sagte Rogers während einer Rede an der Princeton University. "Ich will einen Vordereingang. Und ich will, dass dessen Tür mehrere Schlösser hat. Große Schlösser." So könnte neben dem "Schloss", mit dem ein Kunde auf verschlüsselte Daten zugreifen kann auch ein "Schloss" eingerichtet werden, das der Anwesenheit zweier Teilschlüssel bedarf, zum Beispiel des Geheimdienstes und der jeweiligen Firma. Theoretisch wären auch mehrere Teilschlüssel denkbar, die zum Beispiel einem Aufsichtsgremium gehören.

### Mehrere Ansätze sind denkbar

Doch das ist nur eine der Ideen, die derzeit im Weißen Haus diskutiert werden. Eine andere sieht laut "Washington Post" vor, dass Unternehmen auf richterlichen Beschluss hin verpflichtet werden könnten, beispielsweise die E-Mail- oder Chat-Accounts eines Anwenders zu spiegeln, so dass Ermittler deren Nachrichten mitlesen können.

Ebenso ist angedacht worden, Unternehmen in solchen Fällen dazu zu verpflichten, Backups von auf dem Smartphone gespeicherten Daten anzufertigen, bereits bevor diese Daten verschlüsselt werden.

Derzeit soll geplant sein, US-Präsident Obama noch im April mehrere denkbare Ansätze zur Entschlüsselung von Daten vorzustellen. Dabei gehe es jedoch in erster Linie darum, dem Präsidenten vor Augen zu führen, was technisch möglich wäre.

Dass es in nächster Zeit ein neues US-Gesetz zur Datenverschlüsselung geben wird, ist laut "Washington Post" aber unwahrscheinlich: Ein geteilter Kongress, die neuen Datenschutzbedenken nach den Snowden-Leaks, die Internationalität der Dateninfrastrukturen und nicht zuletzt technische Risiken dürften einer solchen Gesetzgebung im Wege stehen.

*kno*

**URL:**

http://www.spiegel.de/netzwelt/netzpolitik/nsa-neue-plaene-um-an-verschluesselte-daten-zu-kommen-a-1028284.html