Online-Durchsuchungen

Sicherheitslücken als Chance und Gefahr

Tagesschau.de / Stand: 28.07.2021 17:46 Uhr

Ermittlungsbehörden nutzen bei Online-Durchsuchungen zur Verbrechensbekämpfung technische Sicherheitslücken, die Telekom-Firmen offenhalten müssen. Diese sind aber auch Einfallstor für Kriminalität und Spionage. Eine Lösung hat die Politik bislang nicht.

Von Sabina Wolf, BR

Polizei, Verfassungsschützer und Nachrichtendienste dürfen neuerdings verschlüsselten Nachrichtenaustausch zum Beispiel bei Messenger-Apps im Rahmen der sogenannten Quellen-Telekommunikationsüberwachung abhören oder mitlesen. Sie dürfen die Ende-zu-Ende-Verschlüsselung knacken, wenn es um Terrorismus, Mord oder schwere Drogendelikte geht. Die Anordnung einer solchen Maßnahme muss von einem Gericht angeordnet werden. Bewusst offen gehaltene Sicherheitslücken gefährden allerdings die gesamte IT-Infrastruktur, machen Bürgerdaten und die Wirtschaft angreifbar.

Für die Telekommunikationsüberwachung muss ein Programm auf die digitalen Endgeräte der Verdächtigen, meist Handys, aufgespielt werden. Genau diese Sicherheitslücken, nutzen jedoch auch Kriminelle und Geheimdienste.

"Online-Durchsuchung und Quellen-TKÜ, also die Überwachung verschlüsselter Kommunikation, sind massive Eingriffe in die Bürgerrechte, bei denen sich der Staat als Hacker betätigt und IT-Sicherheitslücken ausnutzt, die er eigentlich schließen müsste", beklagt Stephan Thomae, stellvertretender Fraktionsvorsitzender der FDP im Deutschen Bundestag und Mitglied im Parlamentarischen Kontrollgremium (PKGr), das für die Kontrolle der Nachrichtendienste zuständig ist. Sicherheitslücken zu schließen, müsse Priorität haben. Denn die IT-Sicherheit ist die Achillesferse der Gesellschaft so Thomae.

"Einladung an Kriminelle"

Erst am 8. Juni bestätigte das Bundesverfassungsgericht eine grundsätzliche aktive Schutzpflicht des Staates. Demnach hat der Staat eine Verantwortung für die Sicherheit informationstechnischer Systeme und muss diese vor Angriffen durch Dritte schützen. Dass dies nur mit einem umfassenden Schwachstellenmanagement möglich ist, darauf weisen IT-Sicherheitsexperten seit Jahren hin.

Das bewusste Offenhalten von Sicherheitslücken sei nichts anderes als eine Einladung an Kriminelle und fremde Mächte zu Cyberangriffen, Datenklau, Ransomware-Attacken und Spionage, sagt Thomae. Die Sicherheitspolitik von Union und SPD werde selbst zum Sicherheitsrisiko.

Juristisch zweifelhaft

Für Konstantin von Notz, stellvertretender Fraktionsvorsitzender der Bündnis 90/ Die Grünen im Bundestag ist es höchst zweifelhaft, ob die neuen Befugnisse für den Einsatz von Staatstrojanern vor dem höchstem Gericht überhaupt Bestand haben werden: "Bis heute handeln staatliche Stellen mit Sicherheitslücken, die immer auch Kriminellen offenstehen und die IT-Sicherheit von Millionen Menschen in Deutschland, Europa und der Welt gefährden." Ein immer wieder versprochenes, auch vom Bundesverfassungsgericht gerade noch einmal gefordertes gesetzliches "Schwachstellen-Management" habe man nicht eingeführt, so von Notz.

Jens Zimmermann, digitalpolitischer Sprecher der SPD-Bundestagsfraktion räumt auf Anfrage ein, es könne nicht ausgeschlossen werden, dass auch Dritte offene und nicht gemeldete Schutzlücken ausnutzten**.** Die grundrechtliche Schutzpflicht verlange eine Regelung dazu, wie die Behörde den Zielkonflikt zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter IT-Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Strafverfolgung oder Gefahrenabwehr dienenden Quellen-TKÜ anderseits grundrechtskonform auflösen kann. Ein solch zwingend gebotenes Schwachstellenmanagement habe die SPD innerhalb der Großen Koalition leider nicht durchsetzen können.

Rechtmäßige Überwachung zur Verfolgung schwerster Straftaten

Der stellvertretende Vorsitzender der CDU/CSU-Bundestagfraktion, Thorsten Frei, sieht zum Staatstrojaner keine Alternative: "Die einzige Alternative zum Einsatz einer Überwachungssoftware wäre im Grunde nur, dass wir die Kommunikationsdienste verpflichten müssten, uns die Kommunikation der Betroffenen unverschlüsselt auszuleiten." Dies würde bedeuten, dass verschlüsselte Kommunikationsdienste jederzeit unbemerkt einen dritten stillen Kommunikationsteilnehmer in einen Ende-zu-Ende-verschlüsselten Chat einschleusen könnten, um die dort geführte Kommunikation unbemerkt mitzulesen.

Die nächste Bundesregierung wird um die Etablierung eines gesetzlich geregelten Schwachstellenmanagements nicht herumkommen. Dabei gilt es dann, die Schwachstellennutzung, die im Interesse der Sicherheitsbehörden ist, mit der Gefährdung der IT-Sicherheit für die Allgemeinheit abzuwägen. Denn um schwerste Straftaten zu verfolgen und schwerste Gefahren abzuwehren, muss die rechtmäßige Überwachung verschlüsselter Telekommunikation möglich sein. Dies zeigt unter anderem der brutale Mord an dem niederländischen Journalisten Peter R. de Vries.