

Staat als Hacker? NGOs warnen vor katastrophaler Überwachungsgesetzgebung!

Datenschützer warnen vor geplanter Messenger-Überwachung. Offener Brief fordert Stopp des Gesetzes im Nationalrat.



Dolomitenstadt, Österreich - In einer aktuellen Debatte über die geplante Überwachung von Messenger-Diensten haben Datenschützer und NGOs Alarm geschlagen. Der Gesetzesentwurf, der zwischen Mittwoch und Freitag im Nationalrat beschlossen werden soll, wird als „historischer Rückschritt für die allgemeine Sicherheit“ kritisiert. Über 40 Organisationen, darunter renommierte Datenschutzgruppen wie epicenter.works, Greenpeace und die Katholische Aktion, haben einen offenen Brief an alle Nationalratsabgeordneten gerichtet, um gegen die sogenannte „Gefährder-Überwachung“ zu protestieren. Sie warnen vor den Gefahren einer solchen

Gesetzgebung für die individuelle Freiheit und Privatsphäre.

Ein zentrales Argument der Kritiker ist die fehlende unabhängige Kontrolle, da das Innenministerium sich selbst kontrollieren würde. Technisch sei eine gezielte Überwachung von Messenger-Diensten nur möglich, wenn das gesamte Gerät angegriffen wird, wodurch der Staat quasi selbst zum Hacker würde. Diese Vorgehensweise könnte Sicherheitslücken absichtlich offenlassen und erhebliche Folgen für alle Nutzer:innen haben. Laut den NGOs könnte dies besonders schwerwiegende Folgen für Journalisten, Aktivisten, Wissenschaftler und oppositionelle Kräfte haben.

Internationale Beispiele der Überwachung

Das Risiko einer solchen Überwachung ist nicht theoretisch. In anderen Ländern haben sich bereits alarmierende Entwicklungen gezeigt. In Spanien wurde der Geheimdienst beschuldigt, mit der Spionagesoftware „Pegasus“ Mobiltelefone von Katalanen, Journalisten und Regierungsmitgliedern zu überwachen. Ähnlich verliefen die Ereignisse in Griechenland während des sogenannten „Predatorgate“-Skandals, bei dem Politiker und Journalisten ins Visier genommen wurden. In Polen nutzen die Behörden Pegasus gegen fast 600 Personen, darunter viele Oppositionelle und Juristen.

Diese Beispiele zeigen nicht nur das Potenzial für einen Missbrauch von Technologien zur Überwachung, sondern auch die Gefahren für demokratische Strukturen. Die Messenger-Überwachung wurde von der ÖVP als Forderung ins Regierungsprogramm aufgenommen. Nach anfänglichen Unstimmigkeiten über die Verfassungstauglichkeit einigte man sich schließlich auf einen Gesetzesentwurf, dessen Unterstützung durch die Regierungsparteien im Nationalrat jedoch ungewiss ist.

Technologische Risiken durch

Spionagesoftware

Die Diskussion um die Überwachung wird zusätzlich durch die Technologie hinter Spionagesoftware wie „Pegasus“ verstärkt. NSO Group, ein israelisches Unternehmen, hat die Software entwickelt, die in der Lage ist, die Verschlüsselung von Plattformen wie WhatsApp, Signal und Telegram zu umgehen. Laut Berichten kann Pegasus weltweit über 50.000 Telefonnummern überwachen, und sie gibt Hackern umfassenden Zugriff auf Smartphones, einschließlich Kamera und Mikrofon.

Experten betonen, dass die größte Schwachstelle tatsächlich das Endgerät selbst ist, nicht die Verschlüsselungsmethoden an sich. Die Bundesregierung plant sogar, die Verschlüsselung durch den Bundestrojaner zu schwächen, um die Kommunikation über geschützte Messenger zu überwachen. Diese Maßnahmen könnten die Gesamtsicherheit der Verschlüsselung in Frage stellen und schwerwiegende Konsequenzen haben.

Die Bedeutung des Datenschutzes wird in diesem Kontext besonders deutlich. Datenschutzgesetze, wie die Datenschutz-Grundverordnung (DSGVO) der EU, wurden eingeführt, um den Schutz personenbezogener Daten zu gewährleisten und Missbrauch zu verhindern. Prinzipien wie die Verarbeitung personenbezogener Daten nur mit einer zulässigen Rechtsgrundlage und das Recht auf Auskunft und Löschung sollen sicherstellen, dass die Privatsphäre der Nutzer respektiert wird. Es wird jedoch darauf hingewiesen, dass die Entwicklungen in der Technologie und deren Umgang durch die Regierungen ständig neue Herausforderungen an den Datenschutz stellen.

Die NGOs hoffen, dass der offene Brief weitere Abgeordnete mobilisieren kann, um gegen den drohenden Gesetzesbeschluss vorzugehen. Die Sorgen der Experten und Aktivisten über den Datenschutz sowie die Bedrohung durch staatliche Überwachungssysteme sind in der heutigen digitalen Welt relevanter denn je.

Details	
Vorfall	Cyberkriminalität
Ort	Dolomitenstadt, Österreich
Quellen	<ul style="list-style-type: none">• www.dolomitenstadt.at• mobil.stern.de• www.cyberriskmanager.de

Besuchen Sie uns auf: die-nachrichten.at