3834/J
vom 24.10.2025 (XXVIII. GP)

Anfrage

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

an den Bundesminister für Inneres

betreffend: Gibt es Kontakte zur Überwachungsfirma First Wap im Innenministerium?

BEGRÜNDUNG

Eine verdeckte Recherche eines internationalen Journalistennetzwerks – darunter ZDF, Der Spiegel, Der Standard und Lighthouse Reports – hat kürzlich offengelegt, wie mit der Spionagesoftware des Unternehmens First WAP Politiker:innen, Journalist:innen und Prominente getrackt wurden.[1] Das Unternehmen mit Hauptsitz in Indonesien wurde von dem Österreicher Josef Fuchs gegründet und steht aktuell unter deutsch-österreichischer Führung.

Über das First-WAP-Produkt Altamides wurden den Recherchen zufolge jahrelang Mobiltelefone in aller Welt geortet und teilweise auch Kommunikation abgefangen. Das System nutzte keine klassische Spyware auf den Geräten, sondern griff über Mobilfunkinfrastrukturen zu. Es basiert auf sogenannten SS7- und Signalling-Protokollen, die Mobilfunkanbieter untereinander verwenden, um etwa Roaming oder SMS-Zustellung zu ermöglichen. Wer Zugriff auf diese Netzebene hat, kann den Standort von Handys präzise ermitteln oder Kommunikationsmetadaten abfragen – und bleibt dabei für Betroffene unsichtbar.

Ausgewertete Daten zeigen über 1,5 Millionen Ortungsversuche in 168 Ländern – auch in Österreich! Unter den überwachten Personen finden sich Journalist:innen, Politiker:innen, Manager:innen, Künstler:innen – etwa der österreichische Sänger Wolfgang Ambros – und auch kirchliche Würdenträger. Besonders betroffen sind offenbar auch 20 aktive und ehemalige Mitarbeiter:innen des Red Bull Mediahouse, deren Standorte über Handys lokalisiert wurden. Firmentelefone sind ebenso dabei wie private Geräte, Festangestellte genauso wie freie Mitarbeiter. Unter den vermutlich Überwachten bei Red Bull sind auffallend viele hohe Entscheidungsträger, darunter Positionen wie "Head of Legal", "Head of Sport", "Head of Audio", "Head of Marketing" oder "Global Head of Media Technology & IT". Einige der mutmaßlich Betroffenen sind noch immer in exponierten Positionen, unter ihnen auch der heutige Chef des Red Bull Verlags.[2]

---

[1] https://www.derstandard.at/story/3100000291834/big-brother-aus-oesterreich-die-firma-die-handys-weltweit-ueberwachte

[2] https://www.derstandard.at/story/3100000291960/mitarbeiter-des-red-bull-konzerns-wurden-illegal-getrackt-aber-von-wem

In Undercover-Gesprächen sollen Vertreter von First WAP zudem erklärt haben, dass auch der Zugriff auf WhatsApp-Konten „einfach" sei. So könnten Registrierungs-SMS oder Anrufe umgeleitet werden, um so Messenger-Accounts zu übernehmen.

Generell entwickelt sich Österreich unter der aktuellen Bundesregierung vermehrt Richtung Überwachung von Bürger:innen. So wurde im Juli die Messenger-Überwachung beschlossen.[3] Im August hat das Innenministerium die Verfünffachung der Videoüberwachung angekündigt.

Auch vor diesem Hintergrund ist die Frage der für Überwachungsaktivitäten zum Einsatz kommenden Mittel höchst relevant.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Besteht ein Kontakt Ihres Ressorts oder nachgeordneter Dienststellen zu First WAP oder zu verbundenen Unternehmen?
    a) Wenn ja, zu welchen Unternehmen, zu welchem konkreten Zweck und wie ist der Kontakt zustande gekommen?

2) Bestehen oder bestanden Geschäftsbeziehungen Ihres Ministeriums oder nachgeordneter Dienststellen zu First WAP oder zu verbundenen Unternehmen?
    a) Wenn ja, mit welchen Unternehmen, welche Leistungen werden erbracht und seit wann?
    b) Wie hoch sind die Kosten, die dafür entstehen?
    c) Gibt es eine Datenschutz- und Technologiefolgenabschätzung?
    d) Können Sie sicherstellen, dass es zu keinem Abfluss geschützter Daten kam oder kommt?

3) Kam es im Innenministerium oder in nachgeordneten Dienststellen zu einer Teststellung oder Produktpräsentation von Applikationen von First WAP oder verbundenen Unternehmen?
    a) Wenn ja, zu welchem konkreten Zeitpunkt?
    b) Wie ist die Teststellung zustande gekommen?
    c) Welche Applikationen wurden für welche Zwecke vorgestellt und/oder getestet?
    d) Welche Datensätze oder Datenbanken wurden bei der Teststellung verwendet?
    e) Wurden die Grundsätze des Datenschutzes dabei beachtet?

[3] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2025_I_54/BGBLA_2025_I_54.html

f) Gibt es Aktenvermerke zu einer Teststellung?
g) Wie hoch sind die voraussichtlichen Kosten (Anschaffung, Schulungskosten etc)?
h) Gibt es eine Datenschutz- und Technologiefolgeabschätzung?

4) Ist der Einsatz von First WAP Produkten im Zusammenhang mit der Gefährder-Überwachung iSd Novelle zum Staatsschutz- und Nachrichtendienstgesetz möglich oder können Sie ausschließen, dass Produkte von First WAP dafür genutzt werden?

5) Welche Hintergrundchecks sind für potenzielle Vertragspartner vorgesehen, die dem Innenministerium Software anbieten?

6) Waren dem BMI die Fälle der Überwachung von Personen in Österreich vor Offenlegung der Recherche durch das obengenannte Journalistennetzwerk bekannt?

a. Falls ja, wie viele Fälle der Überwachung mit First WAP in Österreich sind Ihnen bekannt?
b. Wie viele Fälle der Überwachung mit anderen Spionagesoftwares in Österreich sind Ihnen bekannt?
c. Falls nein, ermitteln Sie diese Fälle jetzt?

7) Wurde geprüft, ob sich der Gründer oder die Geschäftsführer von First WAP in einem österreichischen Unternehmensregister finden und ob etwaige Kontakte zu staatlichen Stellen bestehen?

8) Gibt es innerhalb des Innenministeriums eine Stelle, die für die Prüfung von Überwachungssoftware von Telekommunikationsbetreibern auf Rechtskonformität zuständig ist?

9) Gab oder gibt es eine Kooperation mit ausländischen Sicherheitsbehörden, Nachrichtendiensten oder Polizeien im Zusammenhang mit der Firma First WAP oder ähnlichen Technologien?

10) Wurde geprüft, ob das Innenministerium selbst Ziel der Überwachung durch First WAP war oder ist?

11) Welche Maßnahmen wurden gesetzt, um die Mobilkommunikation von Mitarbeiter:innen des BMI gegen SS7-basierte Angriffe zu schützen?

12) Gibt es Richtlinien oder technische Standards für den Schutz vor Signalling-Angriffen im Bereich der ministeriellen IT-Sicherheit?

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-24T12:51:29+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	