7388/J
vom 22.10.2026 (XXVIII. GP)

Anfrage

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

an den Bundesminister für Inneres

betreffend Verbreitung von Spyware über Online-Werbung („AdFection") und mögliche Betroffenheit österreichischer Stellen

BEGRÜNDUNG

Am 15. Oktober 2026 hat das Citizen Lab der Universität Toronto den Bericht „Exposing AdFection. How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware" veröffentlicht.[1] Darin wird erstmals öffentlich ein konkreter Angriff nachgewiesen, bei dem kommerzielle Spyware über gezielt ausgespielte Online-Werbung auf Geräte gelangt ist. Die Betroffenen mussten dafür nichts anklicken. Es genügte, dass die Anzeige in einer App oder auf einer Website geladen wurde.

Laut Bericht tritt das Unternehmen Discover-Tech als gewöhnlicher Werbeanbieter auf, dient aber vor allem dazu, Herstellern von Überwachungssoftware Zugang zum Online-Werbemarkt zu verschaffen. Über die Plattform „Controlium" können Kund:innen einzelne Personen anhand ihrer Werbe-ID oder IP-Adresse auswählen und ihnen beim Anzeigen einer Werbung Schadcode zuspielen. Nachgewiesen wurde dies unter anderem bei mindestens 45 Geräten eines internationalen Nachrichtensenders, die mit Spyware des Herstellers Candiru (inzwischen „Integrity Labs") infiziert wurden. Der Bericht dokumentiert außerdem Verbindungen zu den Überwachungsfirmen Bindecy und Intelos.

Die Auswertung von fast vier Milliarden Gebotsdatensätzen zeigt, dass Anzeigen dieser Firma allein zwischen März und Juni 2026 auf fast 200.000 Websites und Apps ausgespielt wurden, darunter weit verbreitete Messenger, Lern- und Wetter-Apps. Anzeigen wurden auch in Netzen des Europäischen Parlaments, der Europäischen Kommission, des Rates der EU, der NATO, der Vereinten Nationen sowie in Ministerien, Streitkräften, Polizeibehörden und bei Betreibern kritischer Infrastruktur zahlreicher Staaten ausgespielt. Eine parallel veröffentlichte Untersuchung des Sicherheitsunternehmens Confiant fand zudem Hinweise auf Ausspielungen im Netz der Internationalen Atomenergie-Organisation mit Sitz in Wien.[2] Eine angezeigte Werbung bedeutet nicht automatisch eine Infektion. Citizen Lab hält aber ausdrücklich fest, dass zumindest eine Profilbildung erfolgte und dringend zu prüfen ist, ob Personen in diesen Netzen infiziert wurden.

Der Bericht beschreibt darüber hinaus einen Akteur, der Schwachstellen bei Mobilfunkbetreibern in über 30 Ländern ausnutzt, um Werbe-IDs mit Telefonnummern zu verknüpfen und Nutzer:innen so massenhaft zu deanonymisieren. Die Untersuchung ist nach Angaben von Citizen Lab nicht abgeschlossen und beruht nur auf einem Ausschnitt der Daten.

Österreich wird im Bericht bei den Regierungsnetzen nicht genannt. Angesichts der unvollständigen Datenlage, der Ausspielungen in EU-Institutionen und in einer internationalen Organisation in Wien sowie der Tatsache, dass die betroffenen Apps und Websites auch in Österreich millionenfach genutzt werden, ist eine Betroffenheit österreichischer Stellen und Personen aber keineswegs ausgeschlossen. Zugleich stellt sich die Frage, ob österreichische Behörden selbst auf Werbedaten gestützte Überwachungswerkzeuge nutzen oder angeboten bekommen haben.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Seit wann ist Ihrem Ressort, insbesondere der Direktion Staatsschutz und Nachrichtendienst (DSN), der Bericht des Citizen Lab bekannt?
2) Wurde der Bericht ausgewertet? Wenn ja, mit welchem Ergebnis?
3) Lagen Ihrem Ressort bereits vor dem 15. Oktober 2026 Erkenntnisse über die Verbreitung von Spyware über Online-Werbung vor? Wenn ja, seit wann und welche?
4) Wurden die im Bericht veröffentlichten technischen Indikatoren (Domains, Server, Signaturen des Schadprogramms) in die Erkennungs- und Schutzsysteme Ihres Ressorts übernommen? Wenn nein, warum nicht?
5) Wurden diese Indikatoren an andere Bundesministerien, die Länder, die Parlamentsdirektion sowie an Betreiber wesentlicher und wichtiger Einrichtungen weitergegeben? Wenn ja, wann und an wen? Wenn nein, warum nicht?
6) Hat Ihr Ressort Kontakt zum Citizen Lab, zu Confiant oder zu Partnerbehörden anderer Staaten aufgenommen, um weitere Informationen zu erhalten? Wenn nein, warum nicht?
7) Liegen Hinweise vor, dass Anzeigen von Discover-Tech in Netzen Ihres Ressorts ausgespielt wurden? (Aufschlüsselung nach Zentralstelle und nachgeordneten Dienststellen)
8) Liegen Hinweise vor, dass solche Anzeigen in Netzen anderer Bundesministerien, oberster Organe oder des Parlaments ausgespielt wurden?
9) Liegen Hinweise vor, dass solche Anzeigen in Netzen von Betreibern kritischer Infrastruktur bzw. wesentlicher und wichtiger Einrichtungen ausgespielt wurden?

10) Sind Fälle bekannt, in denen Geräte in Österreich über Online-Werbung mit Spyware infiziert wurden oder ein entsprechender Verdacht besteht?

11) Sind Fälle bekannt, in denen Journalist:innen, Politiker:innen oder Mitarbeiter:innen von NGOs in Österreich auf diese Weise ins Visier genommen wurden?

12) Wurden Untersuchungen eingeleitet, um eine mögliche Betroffenheit österreichischer Stellen zu klären? Wenn ja, mit welchem Stand? Wenn nein, warum nicht?

13) Gab es Austausch mit internationalen Organisationen mit Sitz in Wien, insbesondere der Internationalen Atomenergie-Organisation, zu einer möglichen Betroffenheit? Wenn ja, mit welchem Ergebnis?

14) Wurden im Zusammenhang mit den im Bericht beschriebenen Vorgängen Ermittlungen durch Sicherheitsbehörden eingeleitet oder Anzeigen erstattet? Wenn nein, warum nicht?

15) Ist Ihrem Ressort bekannt, ob in Österreich tätige Mobilfunkbetreiber von den im Bericht beschriebenen Schwachstellen betroffen sind, über die Telefonnummern mit Werbe-IDs verknüpft werden können?

16) Welche Maßnahmen werden in Abstimmung mit den zuständigen Stellen und den Mobilfunkbetreibern gesetzt, um solche Schwachstellen zu schließen?

17) Haben Dienststellen Ihres Ressorts jemals Produkte oder Dienstleistungen von Discover-Tech, Candiru bzw. Integrity Labs, Bindecy oder Intelos beschafft, getestet, vorgeführt bekommen oder angeboten bekommen? (Aufschlüsselung nach Unternehmen, Zeitpunkt und Produkt)

18) Gab es Kontakte zu diesen Unternehmen oder deren Vertreter:innen auf Messen, bei Produktvorführungen oder über Zwischenhändler? Wenn ja, wann und in welchem Rahmen?

19) Setzt Ihr Ressort Werkzeuge ein, die Werbedaten, Werbe-IDs oder Daten aus Werbeauktionen (Real-Time Bidding) zur Ortung, Identifizierung oder Profilbildung von Personen nutzen? Wenn ja, welche, seit wann und auf welcher Rechtsgrundlage?

20) Hat Ihr Ressort Daten aus Werbenetzwerken oder von Datenhändlern zugekauft oder bezieht es solche Daten über Dritte? Wenn ja, welche, in welchem Umfang und auf welcher Rechtsgrundlage?

21) Wird Online-Werbung auf Dienstgeräten und im Netz Ihres Ressorts technisch blockiert? Wenn ja, seit wann und in welchem Umfang? Wenn nein, warum nicht?

22) Gibt es Vorgaben, Werbe-IDs auf dienstlichen Mobilgeräten zu deaktivieren? Wenn nein, warum nicht?

23) Welche Vorgaben bestehen für die Installation von Apps auf dienstlichen Mobilgeräten, insbesondere von werbefinanzierten Apps?

24) Werden besonders gefährdete Bedienstete, etwa im Kabinett oder in Führungsfunktionen, mit gehärteten Geräten ausgestattet bzw. werden

Schutzfunktionen wie der Blockierungsmodus (Lockdown Mode) verpflichtend aktiviert? Wenn nein, warum nicht?

25) Wurden die Bediensteten Ihres Ressorts nach Veröffentlichung des Berichts gewarnt oder informiert? Wenn nein, warum nicht?

26) Wie viele Sicherheitsvorfälle mit Bezug zu schädlicher Online-Werbung (Malvertising) wurden seit 2023 in Ihrem Ressort registriert? (Aufschlüsselung nach Jahren und Art des Vorfalls)

27) Welche Warnungen oder Empfehlungen hat Ihr Ressort als für Cybersicherheit zuständiges Ressort an andere Ressorts und die Länder herausgegeben?

28) Gibt es Empfehlungen für Medienhäuser, NGOs und die Bevölkerung, wie sie sich gegen Angriffe über Online-Werbung schützen können?

29) Wird die Bedrohung durch Spyware über Online-Werbung im nächsten Lagebild Cybersicherheit bzw. im Verfassungsschutzbericht behandelt? Wenn nein, warum nicht?

30) Gab es zu den Vorgängen Austausch mit Europol, ENISA oder Partnerdiensten anderer Mitgliedstaaten? Wenn ja, mit welchem Ergebnis?

31) Welche Position vertritt Ihr Ressort auf EU-Ebene zu Einschränkungen von Real-Time Bidding und Überwachungswerbung aus Sicht der öffentlichen Sicherheit?

32) Unterstützt Ihr Ressort ein EU-weites Verbot des Handels mit und des Einsatzes von kommerzieller Spyware sowie strengere Exportkontrollen? Wenn nein, warum nicht?

33) Wurde bei der Beantwortung dieser Anfrage Künstliche Intelligenz eingesetzt, insbesondere die Anwendungen KAPA oder GovGPT? Wenn ja, in welchen Arbeitsschritten?

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-10-22T11:48:17+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	