

Dringlichkeitsanfrage

der Abgeordneten König-Preuss (Die Linke)

Mögliche Betroffenheit von Thüringer Landesbehörden und Verfassungsorganen durch aktuelle Phishing-Angriffe auf den Messengerdienst Signal

Aktuelle Medienberichte weisen auf eine laufende Phishing-Kampagne gegen Nutzerinnen und Nutzer des Messengerdienstes Signal hin, die sich gezielt gegen Verwaltung, Politik, Verfassungsorgane und weitere sensible Bereiche richtet. Besonders brisant ist, dass nach diesen Berichten das Signal-Konto der Präsidentin des Deutschen Bundestags erfolgreich kompromittiert wurde und Sicherheitsbehörden von zahlreichen weiteren Betroffenen ausgehen, das Nachrichtenmagazin „Der Spiegel“ berichtet von mindestens 300 Betroffenen. Es besteht die Gefahr, dass über derartige Angriffe nicht nur Einzelkommunikation, sondern auch Gruppenchats und damit ganze Kommunikationsnetzwerke ausgelesen werden können. Das Bundesamt für Verfassungsschutz und das Bundesamt für Sicherheit in der Informationstechnik hatten vor entsprechenden Angriffsmethoden gewarnt, die insbesondere auf Social-Engineering-Ansätze abzielen und die Sicherheitsmechanismen der Dienste ausnutzen.

Ich frage die Landesregierung:

1. Welche Erkenntnisse liegen der Landesregierung über mögliche oder bestätigte Betroffenheiten durch die beschriebene Phishing-Kampagne in Thüringen mindestens seit dem Jahr 2026 im Kontext einer Signal-Nutzung vor, insbesondere bei Mitgliedern der Landesregierung, in den Ministerien, in deren nachgeordneten Behörden, in Landesbetrieben sowie in sonstigen Verfassungsorganen und obersten Landesbehörden (bitte Angabe der Fallzahlen erfolgloser und erfolgreicher Angriffe und Kategorie Angriffsziel)?
2. Wurden im Jahr 2026 Warnungen, Lagehinweise oder Handlungsempfehlungen an den in Frage 1 genannten Adressatenkreis in Thüringen im Kontext der Nutzung von Messengerdiensten übermittelt, insbesondere durch das ThüringenCERT (Computer Emergency Response-Team für die Landesverwaltung im Landesrechenzentrum), das Amt für Verfassungsschutz, das für Informationssicherheit zuständige Ressort oder sonstige zentrale Stellen des Landes (wenn ja, bitte darstellen, wann und in welcher Form dies jeweils erfolgte)?
3. Welche konkreten Maßnahmen wurden nach Bekanntwerden der Warnungen veranlasst, um eine mögliche Betroffenheit bei dem in Frage 1 genannten Adressatenkreis durch kompromittierte Messen-

ger-Accounts festzustellen oder auszuschließen, insbesondere hinsichtlich der Überprüfung gekoppelter Geräte, dienstlich genutzter mobiler Endgeräte, Registrierungs- und Zugangssicherungen, Meldewegen bei Verdachtsfällen sowie einer möglichen forensischen oder administrativen Untersuchung kompromittierter Konten oder Geräte?

König-Preuss