Thüringer Landtag
8. Wahlperiode

Drucksache 8/3555
zu Drucksache 8/3329
01.06.2026

D r i n g l i c h k e i t s a n f r a g e

der Abgeordneten König-Preuss (Die Linke)

und

A n t w o r t

des Thüringer Ministeriums für Digitales und Infrastruktur

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.

Das **Thüringer Ministerium für Digitales und Infrastruktur** hat die **Dringlichkeitsanfrage** vom 23. April 2026 namens der Landesregierung mit Schreiben vom 26. Mai 2026 beantwortet:

Vorbemerkung:
Der Signal-Messenger ist im dienstlichen Kontext zur Nutzung in der Landesverwaltung nicht vorgesehen, kann jedoch auf Wunsch der Ressorts hin aus dem Mobile Device Management des Landesrechenzentrums (TLRZ) heraus installiert werden. Die dort verwalteten Softwareprodukte und -versionen werden regelmäßig durch das ThüringenCERT auf ihre Sicherheit hin überprüft, so dass ein zuverlässiger Betrieb technisch sichergestellt wird.

Die in der Dringlichkeitsanfrage benannte Phishing-Kampagne ist der Versuch, mittels Social Engineering die Kontrolle über Signal-Konten zu erlangen, um sensible Chats und Daten mitzulesen. Die technische Infrastruktur des Messengers selbst wurde bei diesem Vorgehen nicht gehackt. Der Angriff nutzt die Unwissenheit der Nutzer über die Kopplungs-Funktion aus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu entsprechende Sicherheitshinweise und Handlungsempfehlungen veröffentlicht, insbesondere zum Umgang mit Geräteverknüpfungen, QR-Codes sowie verdächtigen Kontaktanfragen.

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)?

Druck: Thüringer Landtag, 4. Juni 2026

Antwort:
Aktuell liegen dem Ministerium für Digitales und Infrastruktur (TMDI) keine Informationen vor, dass bei Behörden oder Einrichtungen der Landesverwaltung Personen von der oben genannten Phishing-Kampagne erfasst wurden. Im Ministerium für Inneres, Kommunales und Landesentwicklung (TMIKL) – insbesondere beim Amt für Verfassungsschutz (AfV) beim TMIKL und der Polizei – liegen derzeit ebenso keine Erkenntnisse über mögliche oder bestätigte Betroffenheiten für den in der Fragestellung genannten Personenkreis vor.

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)?

Antwort:
Das ThüringenCERT im TLRZ hat über den für die Landesverwaltung betriebenen Warn- und Informationsdienst am 9. Februar 2026, 20. April 2026, 24. April 2026, 29. April 2026 und zuletzt am 30. April 2026 die Informationssicherheitsbeauftragten der Ressorts sowie weitere nutzende Landesbehörden vor dem laufenden Angriff gewarnt und jeweils aktuelle Informationen dazu bereitgestellt.

Innerhalb des TMIKL erfolgten seit dem 30. Januar 2026 mehrere Warnungen, Lagehinweise und Handlungsempfehlungen.

Bereits der erste Lagehinweis des Bundes auf Basis eines Pressebericht[1] wurde durch die im TMIKL seinerzeit angesiedelte Koordinierungsstelle Cybersicherheit Thüringen an die Informationssicherheitsbeauftragten des Innenressorts allgemeine Verwaltung, des TMIKL sowie die Beauftragten für Informationssicherheit der Polizei und an die Hausleitung mit der Bitte um Sensibilisierung möglicher Nutzer gegeben. Der Innenminister hat hierdurch am 2. Februar 2026 von dem in dem Pressebericht dargestellten Vorgehen über eine Chatanfrage eines vermeintlichen Signal-Supports mit der Aufforderung, einen Verifkations-Prozess zu starten, Kenntnis erlangt.

Am 6. Februar 2026 veröffentlichten das BSI zusammen mit dem Bundesamt für Verfassungsschutz (BfV) einen gemeinsamen Sicherheitshinweis zum Thema „Phishing über Messenger-Dienste“[2]. Beiden Bundesbehörden lagen aktuelle Erkenntnisse vor, denen zufolge ein wahrscheinlich staatlich gesteuerter Cyberakteur Phishing-Angriffe über Messengerdienste wie „Signal“ durchführt. Im Fokus sollen hochrangige Ziele aus Politik, Militär und Diplomatie sowie Investigativjournalistinnen und -journalisten in Deutschland und Europa stehen. Das AfV wurde im Rahmen des regulären Informationsaustausches zwischen den Sicherheitsbehörden über diesen Sicherheitshinweis unterrichtet. Entsprechend dem verbundweit abgestimmten Vorgehen wurden diese Hinweise sowie konkrete Handlungsempfehlungen für das Erkennen und Stoppen einer möglichen Kompromittierung vom AfV am 9. Februar 2026 elektronisch an die Geheimschutzbeauftragten aller Ressorts sowie der Landespolizeidirektion und des Landeskriminalamts mit der Anregung auf Prüfung einer eigenen Betroffenheit sowie Bitte um Rückmeldung gesteuert. Innerhalb des TMIKL wurden aufgrund der Informationen der damaligen Koordinierungsstelle Cybersicherheit Thüringen und des AfV (siehe oben) am 10. Februar 2026 gemeinsam durch den Informationssicherheits- und den Geheimschutzbeauftragten des TMIKL sämtliche Organisationseinheiten im TMIKL sowohl über die konkrete Vorgehensweise der Angreifer, als auch über konkrete Gegenmaßnahmen im Rahmen einer Hausvorlage unterrichtet.

Aufgrund zunehmender Dynamik der Angriffskampagne haben das BSI und das BfV am 17. April 2026 ihre Warnung zu der Phishing-Kampagne über Messengerdienste wie Signal aktualisiert. Am 20. und 22. April.2026 informierte das AfV wiederum die Geheimschutzbeauftragten aller Ressorts. Das BSI hat

1 https://netzpolitik.org/2026/phishing-angriff-zahlreiche-journalistinnen-im-visier-bei-attacke-ueber-signal-messenger/14

2 https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2026/2026-02-06-gemeinsamer-sicherheitshinweis-phishing.html und https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/202602_BfV_BSI.pdf?__blob=publicationFile&v=9

zudem einen „Handlungsleitfaden bei Phishing über den Signal Support“[3] erstellt. Dieser soll Betroffenen helfen, geeignete und notwendige Maßnahmen zu ergreifen, um das eigene Messenger-Konto sowie die Kommunikation mit anderen zu schützen oder mögliche bereits erfolgte Kompromittierungen aufzudecken und zu bereinigen. Die Stabsstelle Cybersicherheit Thüringen im TMIKL informierte hierüber ebenfalls am 20. April 2026 die Informationssicherheitsbeauftragten des Innenressorts und des TMIKL. Sämtlichen Inhabern von Dienstsmartphones wurde noch am selben Tag per E-Mail dieser Handlungsleitfaden mit der Bitte um Beachtung zur Verfügung gestellt.

3. Welche konkreten Maßnahmen wurden nach Bekanntwerden der Warnungen veranlasst, um eine mögliche Betroffenheit bei dem in Frage 1 genannten Adressatenkreis durch kompromittierte Messenger-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?

   Antwort:
   Aufgrund der Form des Angriffs ist es allein dem Nutzer möglich eine Kompromitierung zu erkennen, weshalb die in Antwort zur Frage 2 genannten Informationen in Umlauf gegeben wurden, die den Adressatenkreis befähigten, die im jeweiligen Ressort notwendigen Maßnahmen in Form der Sensibilisierung zu ergreifen.

   Im Vorfeld dieses Angriffs sensibilisierte das TMDI, wie auch die Informationssicherheitsbeauftragten der Ressorts, fortlaufend und präventiv die Mitarbeiter und Funktionsträger in Kampagnen und Schulungen zur Informationssicherheit (Security-Awareness-Kampagnen). Diese Maßnahmen zielen darauf ab, das Bewusstsein von Mitarbeitenden für Risiken im Umgang mit der IT zu schärfen und sicheres Verhalten im digitalen Alltag zu fördern. So war auch das Thema „Social Engineering“ unter anderem bereits im Jahr 2021 ein inhaltlicher Schwerpunkt einer zentralen Informationskampagne für alle Mitarbeiter der Landesverwaltung. Social Engineering ist die Grundlage für gut vorbereitete Phishing-Angriffe, die dann nicht nur bei der Nutzung von Messengern, sondern wesentlich häufiger bei der E-Mail-Kommunikation eingesetzt wird, um die Kommunikation, einzelne Geräte oder Accounts oder die gesamte Infrastruktur zu kompromittieren.

Schütz
Minister

3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Signal-Support/signal-support_node.html