Verfassungsschutz
Baden-Württemberg

Beobachten.
Informieren.
Schützen.

WARNMELDUNG im Zusammenhang mit der Landtagswahl

Angriffe auf Messenger-Dienste

Datum	**Ausgabe**	**Einstufung**
10. Februar 2026	Februar 2026	TLP:CLEAR

Landesamt für Verfassungsschutz
Baden-Württemberg
Cyberabwehr
Taubenheimstraße 85A • 70372 Stuttgart
Telefon 0711 9544 4985
E-Mail Cyberabwehr@lfvbw.bwl.de

Verfassungsschutz
Baden-Württemberg

**Beobachten.
Informieren.
Schützen.**

Angriffe auf Messenger-Dienste

1. Sachverhalt

Die Bundesrepublik Deutschland befindet sich in einer verschärften hybriden Bedrohungslage. Dies hat auch Auswirkungen auf die Wahl zum 18. Landtag von Baden-Württemberg am 8. März 2026. Mandatsträgerinnen und Mandatsträger sowie Kandidatinnen und Kandidaten für ein politisches Mandat stehen dabei besonders im Fokus fremdstaatlicher Akteure. Zukünftige Mitglieder des Landtags können bereits jetzt zur Zielscheibe für Spionage und Cyberangriffe werden, da sie Zugang zu sensiblen Informationen und Daten haben werden. Dies macht sie attraktiv für einen fremden Nachrichtendienst. Deren Aufklärungsziel ist explizit auch die Politik. In den vergangenen Jahren hat sich weltweit gezeigt, dass gerade im Vorfeld von Wahlen ein breites Spektrum an Cyberangriffen zu beobachten ist. Auch aktuelle Erkenntnisse und Berichte mehrerer IT-Sicherheitsorganisationen[1] belegen hier eine signifikante Zunahme von Aktivitäten fremdstaatlicher Akteure, insbesondere solcher mit Verbindungen zu russischen Nachrichtendiensten.

Das primäre Ziel dieser Angriffsoperationen ist zunehmend die Kompromittierung von Kommunikationskanälen wie Signal, WhatsApp oder Telegram. Das strategische Ziel der Angreifer umfasst dabei sowohl den illegalen Informationsabfluss zu Spionagezwecken als auch das Sammeln von sensiblen persönlichen Informationen und Daten. Diese können zudem zur gezielten Verbreitung von Desinformation verwendet werden (siehe hierzu Warnmeldung “Risiken durch KI-gestützte Desinformation und hybride Einflussnahme”[2]).
Da Messenger-Dienste im Alltag ohnehin intensiv genutzt werden, stellen sie derzeit einen bevorzugten Angriffsvektor dar, um ggf. tiefe Einblick in vertrauliche Absprachen und Strategien zu erhalten.

---

[1] https://www.cisa.gov/news-events/alerts/2025/11/24/spyware-allows-cyber-threat-actors-target-users-messaging-applications letztmaliger Aufruf am 10.02.2026
[2] https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/pdf/20260114_Dokument_Checkliste_KI_Risiken_Taskforce_Desinformation.pdf letztmaliger Aufruf am 10.02.2026

2. Vorgehensweise der Angreifer

Die technische Vorgehensweise der Angreifer ist hochgradig adaptiv und zielt oft nicht auf das Brechen der Verschlüsselung selbst ab, sondern auf die Übernahme der Benutzerkonten oder des Endgerätes. Da Messenger-Dienste wie z. B. Signal eine Ende-zu-Ende-Verschlüsselung bieten, umgehen Bedrohungsakteure diese Hürde, indem sie das Benutzerkonto direkt angreifen. Eine gängige Methode ist die Konto-Übernahme des jeweiligen Messengers durch Social Engineering. Hierbei erhalten Zielpersonen Nachrichten von scheinbar vertrauten Kontakten oder vorgeblichen Support-Mitarbeitern, die unter einem Vorwand dazu auffordern, einen per SMS zugesandten Verifizierungscode weiterzugeben. Sobald dieser Code an die Angreifer übermittelt wird, können diese den Messenger-Account auf einem eigenen Gerät registrieren und die Kontrolle übernehmen.

Eine weitaus subtilere, dokumentierte Methode russischer Cybergruppierungen ist der Einsatz von Spyware oder die Kompromittierung verknüpfter Geräte. Die Angreifer versuchen hierbei durch gezieltes Spear-Phishing – also maßgeschneiderte Nachrichten mit thematisch relevanten Inhalten – das Opfer zum Klicken auf einen Link zu bewegen. Dieser Link führt jedoch nicht zur erwarteten Information, sondern initiiert im Hintergrund die Installation von Schadsoftware oder versucht, eine unautorisierte Verknüpfung des Messenger-Accounts mit einem Desktop-Client des Angreifers herzustellen. Ist dies erfolgreich, wird die Ende-zu-Ende-Verschlüsselung ausgehebelt, da der Angreifer als legitimes "drittes Gerät" alle Nachrichten im Klartext mitsynchronisiert übermittelt bekommt, ohne dass das Opfer auf seinem Smartphone eine Unterbrechung bemerkt.

3. Handlungsempfehlungen

Um die Integrität Ihrer Kommunikation zu gewährleisten, ist die Umsetzung technischer und verhaltensbasierter Härtungsmaßnahmen unumgänglich. Die wichtigste technische Barriere ist die Aktivierung der sogenannten "Registrierungssperre" oder "Zwei-Faktor-Authentifizierung" innerhalb der jeweiligen Messenger-App. Diese Funktion zwingt die App dazu, bei jeder Neuinstallation oder Registrierung auf einem neuen Gerät eine von Ihnen definierte PIN abzufragen. Ohne diese PIN können Angreifer Ihren Account selbst dann nicht übernehmen, wenn sie unrechtmäßig Kenntnis des SMS-Verifizierungscodes erlangt haben. Sie finden diese Option in den Sicherheitseinstellungen z.B. von Signal und WhatsApp.

Des Weiteren empfehlen wir Ihnen, regelmäßig, idealerweise wöchentlich, die Liste der "Verknüpften Geräte" in Ihren App-Einstellungen prüfen. Sollten Sie dort ein Gerät finden, das Sie nicht eindeutig zuordnen können – etwa einen unbekannten Browser oder ein fremdes Betriebssystem –, sollten Sie die Verknüpfung sofort aufheben und entfernen.

Auf Nutzerebene ist eine erhöhte Wachsamkeit erforderlich: Öffnen Sie unter keinen Umständen Links oder Anhänge, die Sie unerwartet über Messenger-Dienste erhalten, selbst wenn der Absender bekannt scheint, da dessen Gerät bereits kompromittiert sein könnte. Verifizieren Sie die Identität Ihrer wichtigsten Kommunikationspartner physisch oder über einen zweiten Kanal, indem Sie die sogenannten "Sicherheitsnummern" abgleichen. Ändert sich eine Sicherheitsnummer plötzlich, ist dies ein Indikator für eine Neuregistrierung oder einen Man-in-the-Middle-Angriff[3]; in diesem Fall sollten Sie die Kommunikation pausieren, bis die Identität telefonisch oder persönlich geklärt ist. Zudem empfiehlt die Cyberabwehr die Option, Nachrichten automatisch nach einer gewissen Zeitdauer zu löschen ("Verschwindende Nachrichten") zu aktivieren.

[3] Bei diesem Angriff platziert sich ein Angreifer "in der Mitte" der Kommunikation zwischen zwei Kommunikationspartnerinnen oder -partnern und kann ohne deren Wissen Daten (z.B. E-Mails) abfangen, kopieren oder verändern. (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/technischer-Hintergrund-E-Mail-Sicherheit/technischer-Hintergrund-E-Mail-Sicherheit.html, letztmaliger Aufruf am 10.02.2026)

4. Fazit

Die Landtagswahl 2026 kann Zielscheibe geopolitischer Interessenlagen fremder Staaten und deren Nachrichtendienste sein. Die Annahme, dass Messenger-Dienste aufgrund ihrer Verschlüsselung per se sicher sind, ist im Hinblick auf die geschilderten Vorgehensweisen von Angreifern eine Fehleinschätzung, die von professionellen Angreifern ausgenutzt wird. Sicherheit entsteht durch den Dreiklang aus der Verwendung einer vertrauenswürdigen App, der Härtung des Zugangs und einem verantwortungsbewussten Nutzerverhalten. Die Umsetzung der genannten Maßnahmen – insbesondere der Registrierungs-PIN und der Kontrolle verknüpfter Geräte – erhöht die Aufwandsbarriere für Angreifer deutlich

5. Kontakt

Sollten Sie entsprechende Anhaltspunkte bzw. eine Betroffenheit feststellen, steht Ihnen die Cyberabwehr des Landesamtes unter den genannten Erreichbarkeiten zur Verfügung. Bei Kontaktaufnahme kann Ihnen seitens des Verfassungsschutzes Vertraulichkeit zugesichert werden.

Telefon: 0711 9544 4985

E-Mail: Cyberabwehr@lfvbw.bwl.de

Zum Senden verschlüsselter E-Mails finden Sie **hier** unseren öffentlichen PGP-Schlüssel.