Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

Gemeinsamer Sicherheitshinweis | 01/2026 | 06. Februar 2026

Betreff | Phishing über Messengerdienste

Ausgangslage

Dem Bundesamt für Verfassungsschutz (BfV) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen aktuelle Erkenntnisse vor, denen zufolge ein wahrscheinlich staatlich gesteuerter Cyberakteur Phishing-Angriffe über Messengerdienste wie „Signal“ durchführt. Im Fokus stehen hochrangige Ziele aus Politik, Militär und Diplomatie sowie Investigativjournalistinnen und -journalisten in Deutschland und Europa.

Sachverhalte

Ausnutzung legitimer Sicherheits-funktionen

Charakteristisch für diese Angriffskampagne ist, dass weder Schadsoftware eingesetzt noch technische Schwachstellen der Messengerdienste ausgenutzt werden. Stattdessen bedienen sich die Angreifer legitimer Sicherheitsfunktionen der Anwendungen und kombinieren diese mit Social Engineering. Ziel ist es, unbemerkt Zugriff auf Einzel- und Gruppenchats sowie auf Kontaktlisten der betroffenen Personen zu erlangen. Der aktuelle Schwerpunkt der Angriffe liegt auf dem Messengerdienst „Signal“, wobei vergleichbare Vorgehensweisen aufgrund ähnlicher Funktionsprinzipien auch bei „WhatsApp“ denkbar sind.

Beobachtet werden zwei Angriffsvarianten:

VARIANTE 1: Übernahme des Kontos via Sicherheits-PIN

Die Angreifer geben sich als offizielles Support-Team bzw. Support-Chat-Bot des Messenger-dienstes aus („Signal Support“ oder „Signal Security ChatBot“). Sie treten direkt über eine Chatnachricht mit ihrer Zielperson in Kontakt. Der Gesprächseinstieg erfolgt in der Regel über eine angebliche Sicherheitswarnung. Die Angreifer erzeugen zudem unmittelbaren Handlungsdruck, indem sie behaupten, dass ohne sofortiges Handeln der Verlust privater Daten drohe. Nur die Übermittlung der privaten

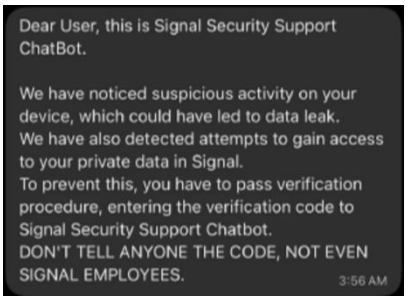

Abb. 1: Gefälschte Support-Nachricht

Sicherheits-PIN der Zielperson oder eines per SMS erhaltenen Verifizierungscodes könne diesen Verlust verhindern. Mit Hilfe der PIN ist es den Angreifern dann möglich, das Nutzerkonto auf einem fremden Gerät, das von ihnen kontrolliert wird, zu registrieren.

Die Angreifer

- übernehmen das Nutzerkonto vollständig und ziehen es auf eine von ihnen kontrollierte Handynummer um,
- erhalten fortlaufenden Zugriff auf Kontaktlisten und neue Nachrichten in Einzel- wie in Gruppenchats,
- erhalten keinen Zugriff auf Nachrichteninhalte vor dem Angriff,
- können im Namen der Zielperson Nachrichten verschicken.

Die Zielperson

- verliert den Zugriff auf ihr Konto,
- wird deshalb unter dem Deckmantel des Support-Chat-Bots mitunter aufgefordert, ein neues Konto zu registrieren.

VARIANTE 2: Unbemerktes Mitlesen via Gerätekopplung über QR-Code

Bei der zweiten Methode machen sich die Angreifer die legitime Funktion zur Kopplung eines zusätzlichen Endgerätes zunutze. Messengerdienste wie „Signal“ oder „WhatsApp“ ermöglichen es ihren Nutzern, ein bestehendes Konto mit weiteren Geräten wie zum Beispiel einem Tablet zu verknüpfen. Die Freigabe des zu koppelnden Gerätes erfolgt durch das Scannen und Bestätigen eines QR-Codes auf dem Primärgerät. Die Angreifer kontaktieren ihre Zielperson unter einem glaubwürdigen Vorwand und bringen sie dazu, einen QR-Code zu scannen. Dieser Code koppelt auch tatsächlich ein neues Gerät mit dem Konto der Zielperson. Allerdings wird dieses Gerät von den Angreifern kontrolliert.

Abb. 2: QR-Code zur Gerätekopplung

Die Angreifer

- erhalten nach erfolgreicher Kopplung fortlaufenden Zugang zu Kontaktlisten und Nachrichten in Einzel- wie in Gruppenchats,
- bekommen zusätzlichen Zugriff auf die Nachrichteninhalte der letzten 45 Tage,
- können im Namen der Zielperson Nachrichten verschicken.

Die Zielperson

- behält weiterhin Zugriff auf ihr Konto,
- bemerkt meist nicht unmittelbar, dass eine fremde Person ihre Kommunikation überwacht.

Bewertung

Spionage als mutmaßliches Ziel

Die aktuell zu beobachtende Angriffskampagne ist insbesondere im Hinblick auf hochrangige Zielpersonen als sicherheitsrelevant einzustufen. Ein erfolgreicher Zugriff auf Messenger-Konten ermöglicht nicht nur die Einsicht in vertrauliche Einzelkommunikation, sondern potenziell auch die Kompromittierung ganzer Netzwerke über Gruppen-Chats. Darüber hinaus lassen sich sensible Kontaktstrukturen rekonstruieren, die für weitergehende nachrichtendienstliche und/oder kriminelle Maßnahmen genutzt werden könnten.

Wahrscheinlich staatlich gesteuerter Akteur

Die geringen technischen Hürden dieser Angriffskampagne führen dazu, dass das Vorgehen gleichermaßen von staatlichen Akteuren mit nachrichtendienstlichem Interesse wie auch von nichtstaatlichen Akteuren, insbesondere von cyberkriminellen Gruppierungen, eingesetzt werden kann. Angesichts der hochkarätigen Zielfläche ist in den derzeit bekannten Fällen wahrscheinlich von einem staatlich gesteuerten Cyberakteur als Urheber auszugehen.

Handlungsempfehlungen

Eine eigene Betroffenheit äußert sich dadurch, dass innerhalb der „Signal“-App darauf hingewiesen wird, dass das eigene Gerät nicht mehr registriert ist, und keine eingehenden oder ausgehenden Nachrichten mehr möglich sind.

Eine Betroffenheit bei einer Kontaktperson kann sich dadurch äußern, dass „Signal“ Sie in Einzel- und Gruppenchats auf eine geänderte Sicherheitsnummer hinweist. Dies sollte zum Anlass genommen werden, bei der betroffenen Person auf einem anderen Kommunikationskanal anzufragen, ob die Änderung legitim oder illegitim war.

Schutzmaßnahmen für potenzielle Zielpersonen:

- Antworten Sie nicht auf „Signal“-Nachrichten von vermeintlichen Support-Konten. Der Kundendienst von „Signal“ meldet sich niemals direkt per „Signal“-Nachricht bei Ihnen.
- Blockieren oder melden Sie Konten, die sich als „Signal“-Support ausgeben.
- Geben Sie Ihre „Signal“-PIN niemals als Textnachricht ein. Legitime PIN-Abfragen erkennen Sie unter anderem daran, dass die Zeichen Ihrer PIN nie im Klartext lesbar, sondern nur durch Punkte oder Sternchen dargestellt sind.
- Aktivieren Sie in „Signal“ unter -> Einstellungen -> Konto die Registrierungssperre.
- Scannen Sie mit der „Signal“-App nur dann QR-Codes, wenn Sie selbst gerade ein Gerät mit „Signal“ verbinden wollen.
- Ignorieren Sie Gruppeneinladungen, die Sie nicht erbeten haben oder von unbekannten Kontakten erhalten.

- Überprüfen Sie regelmäßig die Liste der Geräte, die Zugriff auf Ihr „Signal“-Konto haben. Sie finden diese unter -> Einstellungen -> Gekoppelte Geräte. Entfernen Sie unbekannte Geräte umgehend.

Bitte nehmen Sie bei den folgenden Anzeichen unverzüglich Kontakt zu uns auf:

- Sie haben Ihre „Signal“-PIN oder andere persönliche Informationen an Konten weitergegeben, die als „Signal“-Support aufgetreten sind.
- Sie werden ohne erkennbaren Grund zur Neuregistrierung Ihres Kontos aufgefordert.
- Sie entdecken in der „Signal“-App unter -> Einstellungen -> Gekoppelte Geräte Einträge, die Sie keinem Ihrer regulär genutzten Geräte zuordnen können.
- Nach dem Öffnen eines Links oder dem Scannen eines QR-Codes öffnet sich die „Signal“-App unerwartet oder verhält sich anderweitig ungewöhnlich.
- In „Signal“ werden Nachrichten als gelesen angezeigt, obwohl Sie diese noch nicht gelesen haben.

Weitere Informationen finden Sie unter anderem hier:

- *https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Chat-Messenger/chat-messenger_node.html*
- *https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Chat-Messenger/Messenger/messenger_node.html*

So erreichen Sie uns

Bei Rückfragen sowie für konkrete Sicherheitsanfragen oder Verdachtsfälle kontaktieren Sie uns unter:

Bundesamt für Verfassungsschutz (BfV)
praevention@bfv.bund.de
+49 30 18792-3322

Bundesamt für Sicherheit in der Informationstechnik (BSI)
CERT Bund
certbund@bsi.bund.de
+49 228 999582 5110 (BSI Lagezentrum)

Natürlich steht Ihnen auch die Landesbehörde für Verfassungsschutz in Ihrem Bundesland als Ansprechpartner zur Verfügung. Sollte Ihnen der Kontakt nicht bekannt sein, vermitteln wir Ihnen diesen gerne.

Ihre Angaben werden in jedem Fall vertraulich behandelt.