Signal-Konto gehackt – was tun?

E-Mail-Postfächer, Internet-Accounts, Messenger-Apps - all das kann gehackt werden, mit unangenehmen Folgen. Und es kann alle treffen, bis hin zu Spitzenpolitikern.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesverfassungsschutz warnen vor einer aktiven Phishing-Kampagne unter anderem über Signal mit „hochrangigen Zielen aus Politik, Militär und Diplomatie".

Doch Cyberangriffe treffen längst nicht nur Politiker oder Konzerne. Woran erkennt man, dass man womöglich Opfer wurde? Und was tut man dann?

Laut BSI-Leitfaden versenden die Angreifer Nachrichten, die sich als offizielle Signal-Mitteilungen tarnen. Typische Muster:

- Gefälschter Signal-Chatbot: Eine Nachricht behauptet, Ihr Konto sei gefährdet - und fordert Sie auf, Ihre PIN einzugeben oder sich neu zu registrieren.
- QR-Codes: Ein Link oder QR-Code führt auf eine gefälschte Signal-Seite. Auf dem kleinen Handy-Display fällt die gefälschte URL womöglich nicht sofort auf.
- Geklonte KI-Stimmen und Social Engineering: Angreifer nutzen auch gekaperte Konten, um das Vertrauen von Kollegen und Kontakten auszunutzen und diese gezielt anzugreifen.

Signal gilt als Privatsphäre-orientierter Messenger und wie etwa Threema als Alternative zu WhatsApp - die Phishing-Attacken sind keine Schwäche der App. Die Schwachstelle ist der Nutzer.

FOTO: NICO TAPIA

Was sollten Nutzer unter keinen Umständen tun?

PIN, Registrierungscode oder persönliche Daten an jemanden weitergeben, der sich über Signal als Support, Sicherheitsdienst oder Behörde ausgibt. Signal fragt Sie niemals so nach Ihrer PIN.

Was tun, wenn ich betroffen bin?

Das BSI zeigt Beispiele für Phishing-Nachrichten und erklärt drei Szenarien in einem Leitfaden:

Szenario 1: Ich habe die Nachricht erhalten, aber nicht reagiert

Richtig so. Dennoch: Nachricht löschen, Absender blockieren. Aktivieren Sie anschließend die Registrierungssperre oder Zwei-Faktor-Authentisierung (2FA).

Szenario 2: Ich habe einen Code und/oder PIN eingegeben, aber weiterhin normalen Zugriff auf mein Signal-Konto und wurde nicht zur Neuanmeldung gezwungen

Dann ist Schritt 1: sofort die Signal-PIN über die Einstellungen der App ändern. Schritt 2: Löschen Sie Ihr Messengerkonto über die Einstellungen in der App (Vorsicht: nur das Konto, nicht die App löschen!). Schritt 3: Neues Messengerkonto mit neuer PIN anlegen.

Es sei davon auszugehen, dass den Angreifern nun möglicherweise die eigene Handynummer bekannt ist - wer das aus bestimmten Gründen heikel findet und sichergehen will, besorgt sich in Schritt 4 eine neue Mobilfunknummer und registriert ein neues Messengerkonto mit dieser Nummer.

Schritt 5: Registrierungssperre aktivieren, Mobilfunknummer verbergen und wo immer möglich selbstlöschende Nachrichten aktivieren. Der 6. Schritt: den angeblichen Signal-Support-Kontakt melden und blockieren.

Szenario 3: Ich habe einen SMS-Code und/oder eine PIN eingegeben und keinen Zugriff mehr auf mein Konto.

Der Worst Case - das Messengerkonto ist gehackt. Die Angreifer haben dann das komplette Konto übernommen, können alle Nachrichten und Kontakte einsehen und sich als Sie ausgeben.

Dann: über die App-Einstellungen eine neue und bislang nicht verwendete Signal-PIN vergeben. Kontakte informieren, dass ab dem Zeitpunkt des Angriffs alle Kommunikationen mitgelesen wurden - dafür einen anderen Kommunikationskanal (etwa Telefon, E-Mail) nutzen. Das übernommene Konto muss von Ihren Kontakten unbedingt blockiert werden.

Das gilt auch für Gruppen: Das BSI rät, alle Konten sowie mögliche „gelöschte Konten" aus allen Chat-Gruppen entfernen zu lassen und allen Gruppenmitgliedern mitzuteilen, das übernommene Konto zu blockieren. Es wird dringend empfohlen, die Chat-Gruppen zu löschen und neu zu erstellen; Einladungslinks müssen neu erstellt werden.

Auch hier gilt: Wer sichergehen will, legt Sie sich eine neue Mobilfunknummer zu und registriert damit ein neues Messenger-Konto; und: Registrierungssperre aktivieren, Mobilfunknummer verbergen und wo immer möglich selbstlöschende Nachrichten aktivieren.

Im Anschluss den echten Signal-Support unter https://support.signal.org/hc/de/requests/new kontaktieren, um das alte «verlorene» Konto löschen zu lassen.

Diese Maßnahmen empfiehlt das BSI präventiv, um nicht auf Phishing-Maschen hereinzufallen - nicht nur für Signal:

- Registrierungssperre aktivieren: Einstellungen→ Konto→ Registrierungssperre. Verhindert die Übernahme des Kontos auf einem fremden Gerät.
- Verknüpfte Geräte regelmäßig prüfen: Einstellungen → Verknüpfte Geräte. Alles Unbekannte sofort entfernen.
- Selbstlöschende Nachrichten nutzen: Begrenzt den Schaden, falls Angreifer Zugriff erlangen.
- Niemals PIN oder Registrierungscode weitergeben - auch nicht an vermeintlichen Signal-Support.
- Starke, einzigartige Passwörter für alle Konten nutzen: Das BSI hat dazu und zur Auswahl eines Passwortmanagers Tipps auf seiner Website.
- Zwei-Faktor-Authentifizierung (2FA) aktivieren: Das BSI empfiehlt die 2FA für alle Dienste, die das unterstützen.

Krypto-Gewinne gemacht? Was Sie jetzt versteuern müssen

Egal ob Bitcoin, Tether oder Ethereum: Wer privat mit Kryptowährungen handelt und dabei Gewinne einfährt, muss diese unter Umständen versteuern. Die Frage ist nur: in welchen Fällen? Die Vereinigte Lohnsteuerhilfe (VLH) klärt auf.

Kauf und Verkauf von Kryptowährungen gelten in Deutschland als privates Veräußerungsgeschäft. Solche bleiben steuerfrei, sofern zwischen Anschaffung und Veräußerung mehr als ein Jahr vergeht. Wer innerhalb dieser Frist verkauft, profitiert immerhin noch von einer Freigrenze.

Veräußerungs-Freigrenze von 1.000 Euro pro Jahr - insgesamt

Machen die Gewinne aller privaten Veräußerungsgeschäfte - also zum Beispiel auch aus dem Verkauf von Edelmetallen, Schmuck oder nicht selbst genutzten Immobilien - weniger als 1.000 Euro pro Jahr aus, werden diese ebenfalls von der Steuer verschont.

Verluste aus privaten Veräußerungsgeschäften aus ein und demselben Jahr dürfen mit entsprechenden Gewinnen verrechnet werden. Aber Achtung: Liegt der Gewinn auch nur einen Euro über dieser Freigrenze, muss er komplett versteuert werden - nicht nur der darüberliegende Anteil, teilt die VLH mit.

Dokumentation mit Daten, Kursen, Haltedauer und Kosten

Ganz wichtig: Wer mit Kryptowährungen handelt, muss die Geschäfte penibel und nachvollziehbar als Nachweis fürs Finanzamt dokumentieren. Dazu sind der VLH zufolge unbedingt folgende Daten zu notieren:

- Die Daten für den An- und Verkauf samt dem jeweiligen Kurs
- Die Haltedauer, Anzahl und Bezeichnung der Kryptowerte
- Die Kosten für die Anschaffung und Erlöse aus dem Verkauf

Finanzämter können darüber hinaus weitere Angaben verlangen. Sie tun das laut VLH vor allem dann, wenn Kryptowerte innerhalb einer Wallet umgeschichtet werden oder deren Handel über eine ausländische Plattform erfolgt. (dpa)