Phishing statt Hacking: Threema ordnet die aktuelle Angriffswelle auf Messenger-Nutzer in Politik und Militär ein

Die Phishing-Vorfälle rund um Signal und andere Messenger sorgen international für Schlagzeilen. Im Fokus stehen Schlüsselpersonen aus Militär, Medien und Politik, z.B. Bundestagspräsidentin Julia Klöckner. Warnungen von Sicherheitsbehörden zeigen: Die Angriffe laufen weiter, gewinnen an Dynamik und treffen immer mehr schützenswerte Kommunikationsumgebungen. Threema, ein Marktführer für sichere Kommunikationslösungen, ordnet die Lage ein und zeigt praktische Sicherheitsvorkehrungen auf.

In der Berichterstattung rund um die aktuelle Phishing-Welle ist oft vom sogenannten «Signal-Hack» die Rede. Das ist jedoch irreführend. Die Verschlüsselung von Signal wurde nicht gebrochen. Stattdessen verfolgen die Angreifer eine andere Taktik: Sie greifen nicht den Dienst direkt an, sondern täuschen dessen Nutzer. Die Phishing-Attacke zielt darauf ab, Menschen zur Preisgabe von Verifizierungscodes oder anderen sicherheitsrelevanten Informationen zu bewegen und sie dadurch unfreiwillig zum Einfallstor zu machen.

Danilo Bargen, CTO bei Threema, sagt dazu: «Die aktuellen Vorkommnisse zeigen, dass es gerade bei der Kommunikation in Politik, Militär, Verwaltung oder bei kritischer Infrastruktur nicht ausreicht, Kommunikationsmittel allein an ihrer Verschlüsselung zu messen. Ende-zu-Ende-Verschlüsselung ist eine notwendige Voraussetzung, aber keine hinreichende. Wer sensible Daten schützen will, muss den Kommunikationskanal als Ganzes betrachten und z.B. mit Mechanismen gegen Social Engineering die Benutzer vor sich selbst schützen.»

Worauf es neben der Ende-zu-Ende-Verschlüsselung sonst noch ankommt, lässt sich an drei Punkten illustrieren:

1. Nachvollziehbare Vertrauensstufen für Kontakte

Nutzer müssen sofort erkennen, ob ein Kontakt verifiziert, bekannt oder unbekannt ist. Gerade bei angeblichen Support-Nachrichten oder sicherheitsrelevanten Aufforderungen entscheidet diese Einordnung der Vertrauenswürdigkeit darüber, ob ein Täuschungsversuch auffliegt oder Erfolg hat. Ohne diese Kontaktverifizierung fehlt ein wichtiges Warnsystem.

2. Möglichkeit, die Kontaktaufnahme auf autorisierte Personen zu begrenzen

In sicherheitskritischen Umgebungen sollten unberechtigte Personen nicht einfach Mitarbeitende anschreiben können. Geschlossene Nutzerkreise und klar definierte Kommunikationsräume senken die Angriffsfläche erheblich. Das nimmt Phishing einen grossen Teil seiner Reichweite.

Besonders sensible Organisationen sollten ihre Kommunikationslösung ohnehin selbst hosten. Gemeinsam mit der Infrastruktur sind dann auch Zugriffsberechtigungen und Teilnehmerkreise vollständig unter der eigenen Kontrolle.

3. Keine Benutzerkonten, die an Telefonnummern gebunden sind

Wenn Konten inhärent an Telefonnummern oder E-Mail-Adressen geknüpft sind, entstehen unweigerlich erhebliche Risiken. Ein typisches Beispiel: Ein Angreifer bringt einen Nutzer per Phishing dazu, einen Verifizierungscode weiterzugeben, der an seine Telefonnummer und E-Mail gebunden ist. In diesem Moment kann der Angreifer sich als die Zielperson auf einem anderen Gerät registrieren und deren Identität übernehmen. Insbesondere SMS-basierte

Wiederherstellungsprozesse schaffen hier Angriffsflächen, weil sie wesentlich von der Sicherheit der Mobilfunkinfrastruktur abhängen.

Ein Gegenmodell dazu sind unabhängige Adressierungselemente wie die Threema-ID: Das ist eine zufällige Zeichenfolge ohne inhärenten Personenbezug. Zwar können auch Threema-Nutzer auf Wunsch eine Telefonnummer mit ihrer Threema-ID verknüpfen, aber eine Threema-ID lässt nicht mittels SMS-Verifizierungscode wiederherstellen. Somit sind die gegenwärtigen Phishing-Angriffe nicht durchführbar.

Über Threema

Die Threema GmbH wurde 2014 gegründet und ist eine Pionierin sicherer Instant-Messaging-Lösungen für Organisationen und Private. Der Fokus des Schweizer Unternehmens, das seine eigenen Server in der Schweiz betreibt, liegt auf konsequentem Datenschutz und Datenvermeidung. Die Threema-App ist Open Source und zählt mittlerweile über zwölf Millionen Nutzer in Europa und darüber hinaus. Die Business-Anwendung Threema Work hat sich zum Marktführer im deutschsprachigen Raum entwickelt und wird von über 8’000 Unternehmen, Behörden, Schulen und Verbänden eingesetzt.