2 Multi-Channel-Angriffe auf dem Vormarsch

Cyberkriminelle kombinieren Kanäle in komplexe 3D-Phishing-Angriffe ...

Cyberkriminelle haben ihr Repertoire an Angriffstaktiken und -kanälen in den letzten Jahren in rasantem Tempo vergrößert. **E-Mail ist 56 Prozent der Sicherheitsbeauftragten in der DACH-Region zufolge zwar immer noch der primäre Angriffskanal**.[1] Doch gleichzeitig diversifizieren Angreifende ihre Strategien und nutzen oft für einen einzigen Angriff mehrere Kanäle. Hinzu kommt, dass das Voranschreiten von KI ihnen ermöglicht, schwer aufspürbare und zielgerichtete Angriffe von hoher Komplexität durchzuführen. In unserer Umfrage zu den aktuellen Cybercrime-Trends **berichten 98 Prozent der Organisationen in der DACH-Region von einem Anstieg der Multi-Channel-Angriffe im vergangenen Jahr**.

Die Hintergründe? Angreifende haben es leichter denn je, da wir ständig neue Kommunikationskanäle nutzen. Sie nehmen ihre Zielpersonen durch eine Kombination aus E-Mail und Social Media, Telefonanrufen und Messenger-Apps ins Kreuzfeuer. Damit ahmen sie unsere normalen Kommunikationsmuster nach, was sie glaubhafter wirken lässt, – zum Beispiel, indem sie ein Dokument per E-Mail senden und danach über eine Messenger-App nachfragen, ob ihr Opfer es erhalten hat.[2] Strategien dieser Art, zu denen Phishing, Vishing, Smishing und QR-Phishing gehören, entwickeln sich in komplexe **„3D-Phishing-Angriffe“**.[3] Angetrieben durch KI integrieren sie nahtlos Voice-, Video- und textbasierte Elemente und werden so erschreckend überzeugend. Der in Trend 1 erwähnte Angriff auf den CEO von WPP veranschaulicht diese Vorgehensweise nur zu gut: Die Angreifenden bauen über WhatsApp Vertrauen auf, nutzen Microsoft Teams, um weiter mit ihrem Opfer zu interagieren, und führen danach mittels KI-generiertem Deepfake Anrufe durch, um an sensible Daten und Geld zu gelangen.[4]

... die noch nie so zielgerichtet und schwierig zu erkennen waren

Nicht nur ihr Multi-Channel-Ansatz macht diese Angriffe erschreckend komplex, sondern auch ihre äußerst zielgerichtete Ausführung. Für fortschrittliche Social-Engineering-Methoden wie Pretexting machen sich Cyberkriminelle online verfügbare Informationen über ihre Zielperson zunutze. Um diese realen Angaben herum bauen sie ihre erfundenen Szenarien auf und erschleichen sich so Vertrauen und Glaubwürdigkeit. Diese Art von Angriff wird immer häufiger – laut Verizon **sind weltweit 73 Prozent der Datenschutzverstöße bei Social-Engineering-Angriffen auf Phishing und Pretexting zurückzuführen**.[5]

Diese Angriffsmethoden sind für Zielpersonen wie auch die Behörden schwer zu erkennen, da sie oft über Plattformen mit unzureichenden Schutzmaßnahmen, wie Telegram, durchgeführt werden. Solche Plattformen spielen nicht nur bei der Ausführung von Angriffen, sondern auch bei der Professionalisierung der Cyberkriminalität eine zentrale Rolle. In

1 **SoSafe (2024).** Human Risk Review 2024.
2 **Northdoor (2024).** Phishing Threat Trends Report.
3 **Cyber security insiders (2024).** New Surge in Risky Business Email Compromise Phishing Attacks.