SICHERHEIT

Hybride Angriffe werden zunehmen

In Deutschland ist die Zahl der Betrugsversuche im Jahr 2021 rasant angestiegen. 39 Prozent der Bundesbürger berichteten in einer Bitkom-Studie, dass ihre persönlichen Daten ungefragt weitergegeben wurden. 15 Prozent haben sogar Betrug beim Onlinebanking erlebt. Im Jahr 2022 werden diese Fälle eher noch zunehmen. Fünf Trends in Sachen Sicherheit, auf die sich Finanzdienstleister in diesem Jahr einstellen müssen, hat das Verhaltensbiometrieunternehmen Biocatch ausgemacht.

1. Angreifer werden vermehrt auf hybride Betrugsformen zurückgreifen, um die Sicherheitsmechanismen von Banken zu umgehen. So können sie beispielsweise mit Voice Scamming beginnen, um dann auf den Endgeräten der potenziellen Opfer sogenannte Remote Access Tools zu installieren, die ihnen vollen Zugriff auf die Geräte ihres Opfers erlauben, sodass sie beispielsweise einmalige Passcodes und Anmeldedaten abfangen können. Laut einer Untersuchung von Biocatch wurde im zweiten Quartal 2021 in einem von 24 Betrugsfällen ein Remote Access Tool entdeckt. Das entspricht einem Anstieg von 150 Prozent gegenüber dem Quartal im Vorjahr. Aber auch Kontoübernahmen (Account Take Over) mit anschließendem Scamming werden immer beliebter. Durch das hybride Vorgehen ist es für Cyberkriminelle leichter, an den einzelnen Sicherheitsmaßnahmen vorbeizukommen und diese auszuhebeln. Neben hochorganisierten Cyberkriminellen wird es auch zunehmend für „Hobby-Kriminelle" einfacher, Cyberbetrug zu begehen. Denn Kriminelle bieten im Darknet Betrugskampagnen und die zugehörige Malware als Dienstleistung an. Das Prinzip dahinter ist dasselbe wie bei Software-as-a-Service (SaaS)-Angeboten.

2. Auch Künstliche Intelligenz wird vermehrt eine Rolle bei Betrugsversuchen spielen, vor allem in Form von Betrugsversuchen mit Deepfake Voice, als Social-Engineering-Attacke in Echtzeit, wenngleich die Technologie der stimmlichen Fälschungen noch nicht so ausgereift ist wie Fotos und Videos.

3. Im vergangenen Jahr gab es vermehrt Angriffe durch den vor allem für Android-Geräte konzipierten Banking-Trojaner Flubot auf mobile Endgeräte. Hauptaufgabe der Malware ist es, Bankinformationen des Opfers zu stehlen. Zudem sind der Schadcode in der Lage, Kryptowährungen zu erbeuten und sensible Daten zu exfiltrieren. Viele Banken haben ihre Sicherheitssoftware für diese Art von Malware noch nicht angepasst oder nicht implementiert. Da durch Corona verstärkt mobile Endgeräte für Bankgeschäfte genutzt werden, ist jedoch davon auszugehen, dass Kriminelle verstärkt Malware über Smartphones einschleusen werden. Deshalb sind angepasste Sicherheitsmaßnahmen für Banken und Finanzdienstleister wichtig.

4. Der Druck der Aufsichtsbehörden auf Banken und Finanzinstitute wird zunehmen. Unter anderem werden technische Spezifikationen für automatisierte Identitätsnachweise stärker unter die Lupe genommen, was sich auf Verfahren wie Know-Your-Customer (KYC) und Anti-Money-Laundering (AML) auswirken kann.

5. Der Trend zur passwortlosen Authentifizierung, hauptsächlich über biometrische Verfahren, wird mit dem kundeneigenen Gerät (Besitz) und Inhärenz (Biometrie) nicht mehr nur auf mobile Endgeräte beschränkt sein. Red.