Spoofing, Scamming, Telefonbetrug – Betrugsmaschen 4.0 im modernen Bankalltag

Banken und ihre Kunden sind täglich einer Vielzahl von Betrugsversuchen ausgesetzt. Der folgende Beitrag stellt gängige Betrugsmaschen vor und geht auf mögliche Abwehrmaßnahmen ein.

Die Kriminalität oder besser: die Ausführung krimineller Handlungen hat sich in den letzten Jahren vor dem Hintergrund der zunehmenden Digitalisierung gewandelt.

In der „analogen" Welt werden Diebstahl, Raub, Einbruch und ähnliche Delikte – abhängig vom jeweiligen Zielobjekt – umfangreich und minutiös geplant. An der jeweiligen Tathandlung sind ggf. mehrere Personen (Spezialisten) mit unterschiedlichen Aufgaben beteiligt. Vorhandene Sicherungsmaßnahmen, wie z. B. Einbruchsschutz, Sicherheitspersonal oder Alarmsysteme, müssen überwunden werden. Vorbereitung, Durchführung und „Nachbereitung" folgen einem Plan, der unbedingt einzuhalten ist. Spuren müssen verwischt, Fluchtpläne entwickelt sein.

Gemeinsam ist den Delikten in der analogen Welt der konkrete räumliche Bezug oder Kontakt zwischen Täter und Opfer bzw. Zielobjekt. Geldbörsen müssen vor Ort entwendet, Handtaschen der Eigentümerin entrissen oder Gemälde aus einem Museum gestohlen werden.

In der „digitalen" Welt hingegen ist kein unmittelbarer Kontakt des Kriminellen mit potenziellen Opfern notwendig. Die „Kommunikation" kann ohne räumlichen Bezug und damit deutlich anonymer erfolgen. (Einzel-)Täter können praktisch von überall auf der Welt aktiv werden.

Ein weiterer wesentlicher Unterschied scheint der „Faktor Mensch als (vermeintliche) Schwachstelle" im digitalen System zu sein. Kriminelle müssen in der digitalen Welt nicht mehr stehlen oder rauben – es muss ihnen nur gelingen, andere dazu zu bringen, Geld oder Vermögenswerte „aus freien Stücken" zu übertragen. Hierbei spielen gute Kenntnisse und Informationen über das oder die Opfer (z. B. eine Privatperson oder auch eine Bank), eine „gute" Geschichte und das psychologische Geschick, die emotionale Schwachstelle des digitalen „Gegenübers" unmittelbar zu erfassen, eine bedeutsame Rolle.

Kriminellen gelingt es immer wieder, angeblich besonders dringende Zahlungen mittels telefonischer Überweisungen bei einer Bank auszulösen. Privatpersonen werden dazu gebracht, Geld für Flugtickets oder Arztrechnungen für eine angeblich in Not geratene Person zu zahlen. Ein Klassiker ist nach wie vor, Notarkosten für einen angeblichen Glücksspielgewinn oder eine absurde Nachlassabwicklung überweisen zu lassen.

In diesem Zusammenhang fallen häufig Begriffe wie Spoofing, Scamming, Phishing oder auch der so genannte CEO-Fraud.

Was verbirgt sich hinter diesen Begriffen?

- Beim **SPOOFING** handelt es sich schlicht um das Fälschen von Identitäten im Internet oder per Telefon.

  Täter geben sich als vertrauenswürdige Personen (z. B. Bankmitarbeiter) aus, um an sensible Daten oder Zugangsdaten zu gelangen. Bekannt geworden ist dieses Vorgehen insbesondere durch die Manipulation von Telefonnummern. Ein Krimineller ruft z. B. von außerhalb der EU an. Auf dem Zieltelefon wird die Telefonnummer der Hausbank angezeigt. Zu dieser Betrugsmasche zählt aber auch die so genannte Enkeltrick-Methode.

  Ziel des Spoofings ist es, Geld oder persönliche (Zahlungs-)Daten des Opfers zu erhalten.
- **PHISHING** geht mit dem Spoofing einher. Opfer werden durch gefälschte E-Mails oder Webseiten verleitet, vertrauliche Daten wie Kennwörter oder Kontodaten preiszugeben. Nicht selten enthalten offiziell erscheinende Phishing-E-Mails Dateianhänge, die – werden sie geöffnet – Malware auf dem PC oder Netzwerk installieren.
- **SCAMMING** ist ein Oberbegriff für Internetbetrug im Allgemeinen. Der Scamming-Mechanismus lautet vereinfacht: Zahle wenig, erhalte viel.

  Ziel ist es, Menschen dazu zu motivieren, Geld oder persönliche (Zahlungs-)Daten zu überlassen. Häufig tritt Scamming im Zusammenhang mit vorgetäuschter Liebe (Love-Scamming) oder Gewinn-/Erbschaftsversprechen auf.
- **CEO-FRAUD** ist eine gezielte Betrugsmasche in oder gegen Unternehmen und Banken.

  Dabei geben sich Kriminelle per E-Mail oder Telefon als z. B. Geschäftsführer des eigenen Unternehmens oder – wichtiger für die Bankbranche – eines guten Geschäftskunden aus.

  Mitarbeiter werden unter Zeit- und psychologischem Druck und mit schlüssiger Begründung dazu gebracht, beträchtliche Überweisungen (ins Ausland) zu tätigen.

  Ist erst mal Geld in Richtung Kriminelle geflossen, lässt es sich durch die modernen Zahlungssysteme in Sekundenschnelle an nahezu jeden beliebigen Ort der Welt weiterleiten.

Genaue Zahlen über die Höhe der Schäden, die durch Internetbetrug und CEO-Fraud entstehen, gibt es nicht. Dies liegt auch daran, dass es – wie z. B. beim Love-Scamming – einige Zeit dauern kann, bis Opfer die perfide Übervorteilung erkennen und realisieren. Zudem wird nicht jede Straftat zur Anzeige gebracht. Schätzungen gehen dennoch von Schäden in Milliardenhöhe aus (siehe hierzu auch: BKA-Forschungsbericht: Kosten und Schäden durch Cyber-Kriminalität in Deutschland 1/2024[1]).

Fazit

Die Kriminalität hat sich durch Nutzung digitaler Werkzeuge und moderner Technik verändert. Der in der analogen Welt notwendige räumliche Bezug zwischen Täter und Opfer ist im Internetzeitalter nicht mehr ausschlaggebend. Ganz wesentlich, insbesondere bei der Initiierung von Abwehrmaßnahmen gegen Internetbetrügereien, ist der Faktor Mensch.

Für die Bankenbranche ist es daher von besonderer Wichtigkeit, nicht nur konkrete Sicherungsmaßnahmen weiter zu pflegen und nachzujustieren. Vielmehr sind regelmäßige Mitarbeiter-Schulungen zu den Betrugsmaschen 4.0 und ein Klima von Vertrauen und Sicherheit essentiell, um Betrugsversuche zu entdecken und zu verhindern. Im tatsächlichen Schadensfall gilt es, einen kühlen Kopf zu bewahren und die notwendigen Schritte zur Schadensbegrenzung zügig, aber nicht hektisch, einzuleiten. ▬

Thomas Schröder
Abteilungsleiter Geldwäsche- und Betrugsprävention,
E-Mail: thomas.schroeder@dz-cp.de

[1] Quelle: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2024KKAktuell_Kosten_Schaeden_Cyberkriminalitaet.html