Betrug im Zahlungsverkehr

Bekämpfung mit ganzheitlichem Ansatz

Phishing-Angriffe und Betrugsversuche gehören zu den größten Bedrohungen für die Sicherheit des österreichischen Zahlungsverkehrs. Die Methoden werden dabei auch technologisch immer ausgefeilter und stellen die Institute vor neue Herausforderungen. Die Betrugsbekämpfung ist nur mithilfe intelligenter moderner Methoden zur Automatisierung und zur risikobasierten Echtzeitanalyse darstellbar. Aus Sicht der FMA ist es im Hinblick auf neue gesetzliche Anforderungen essenziell, dass Banken ihre Schwachstellen in diesem Bereich ermitteln und beheben.

Im Jahr 2024 wurden im österreichischen Zahlungsverkehr über 330.000 Betrugsfälle mit einem Gesamtschaden von über € 93 Millionen registriert – Tendenz steigend. Derzeit gängige Betrugsmaschen sind etwa:

- **Identitätsmissbrauch:** Betrüger:innen geben sich als Mitarbeiter:innen von Banken und Behörden aus, um sich unrechtmäßig Zugang zu sensiblen Kundendaten zu verschaffen.
- **Fake-Onlineshops und gefälschte Bankwebseiten:** Fake-Websites, die bekannten Online-Shops oder Marktplätzen nachempfunden sind und zur Eingabe sensibler Daten verleiten.
- **Betrügerisch erlangte eSIM-Karten:** Dadurch werden Sicherheitsmechanismen unterlaufen – insbesondere bei Zwei-Faktor-Authentifizierungen – und Transaktionen manipuliert.

In der aufsichtlichen Praxis der FMA zeigt sich immer wieder, dass Institute, die auf moderne Technologien und klar strukturierte Abläufe setzen, Betrugsversuche frühzeitig erkennen und wirksam bekämpfen können. Besonders wirkungsvoll ist der Einsatz von Transaktionsüberwachungssystemen, die verdächtige Aktivitäten unmittelbar erfassen und automatisiert Gegenmaßnahmen einleiten.

Immer mehr Institute setzen auf Lösungen, die künstliche Intelligenz (AI) und Machine-Learning-Algorithmen nutzen, um frühzeitig Betrugsmuster zu erkennen und potenzielle Risiken gezielt zu minimieren. Dabei erschweren die nunmehr flächendeckend eingeführten Möglichkeiten von Instant Payments einige Maßnah-

§ Meldepflicht gem. § 86 Abs. 3 ZaDIG 2018
Zahlungsdienstleister haben der FMA statistische Daten zu Betrugsfällen in Verbindung mit den unterschiedlichen Zahlungsmitteln vorzulegen. Die FMA hat sicherzustellen, dass diese Daten der EBA und der EZB in aggregierter Form zur Verfügung gestellt werden.

men gegen Betrug, da derartige Zahlungen innerhalb weniger Sekunden ausgeführt werden und eine nachträgliche Rückholung von Beträgen nicht mehr möglich ist. Diese Zahlungsart wird daher in Zukunft genau zu beobachten sein.

Ein wirksames Vorgehen gegen Betrug im Zahlungsverkehr erfordert den koordinierten Einsatz einer Vielzahl unterschiedlicher Maßnahmen. Dazu zählen beispielsweise:

Aufklärung und Kommunikation:
Bei den meisten Betrugsmustern (wie Identitätsmissbrauch oder Fake-Shops) spielt der Faktor »Mensch« eine bedeutende Rolle. Transparente Kund:innenkommunikation (z. B. durch Awareness-Kampagnen) und die Sensibilisierung von Mitarbeiter:innen (z. B. durch gezielte Schulungen) sind daher absolut entscheidend.

Interne Abläufe und Dokumentation:
Klare interne Abläufe und eine lückenlose Dokumentation sind essenziell: Einheitliche interne Richtlinien sowie eindeutige Zuständigkeiten sorgen dafür, dass bei Verdacht auf Betrug rasch gehandelt wird und alle Schritte nachvollziehbar bleiben. Die Etablierung einer zentralen Informationskette, konkreter Zuständigkeiten, sowie die Einrichtung einer Datenbank für die Dokumentation schafft Transparenz und Effizienz im Umgang mit Betrugsfällen.

Holistischer Ansatz:
Ein integrativer Ansatz erweist sich als besonders wirksam: Institute, die technische Maßnahmen wie Transaktionsüberwachung, strukturierte organisatorische Prozesse, gezielte Sensibilisierung der Mitarbeitenden und aktiven Kundenschutz – etwa durch Informationskampagnen, Warnmeldungen oder die Sperrung von Transaktionen während eines Telefonats – gemeinsam umsetzen und regelmäßig evaluieren, bekämpfen Betrugsfälle nachweislich effektiver. Ein kontinuierlicher Austausch zwischen den Fachbereichen für Betrugsprävention, IT-Risikomanagement, Öffentlichkeitsarbeit und Kundenservice schafft die Grundlage dafür, dass sämtliche Maßnahmen innerhalb eines Instituts koordiniert und zielgerichtet zum Schutz vor Betrug eingesetzt werden.

Risikobasierte Echtzeit-Analyse durch KI-gestützte Systeme:
Institute, die Machine-Learning-Modelle zur Erkennung von Betrugsmustern nutzen, erkennen verdächtige Transaktionen häufig früher. Diese intelligenten Systeme reagieren flexibel auf aktuelle Betrugsmuster und Marktentwicklungen, indem sie die Kriterien für die Einstufung auffälliger Transaktionen fortlaufend anpassen und so neue Betrugsversuche zeitnah identifizieren. Ebenso sind Methoden der Verhaltensanalyse zur Erkennung verdächtiger Interaktionen nützlich (wie zum Beispiel ungewöhnliche Login-Zeiten oder Gerätekonstellationen)

Umfassende Eskalationsprozesse:
Institute mit klaren und regelmäßig getesteten Incident-Response-Plänen konnten bei Angriffen deutlich schneller reagieren und Schäden begrenzen.

Stärkere Authentifizierungsverfahren/ Rückrufverfahren:
Neben der verpflichtenden Zwei-Faktor-Authentifizierung hat sich die Aktivierung einer dritten Sicherheitsebene bei verdächtigen Transaktionen als wirksames Mittel gegen Betrug erwiesen (z. B. biometrische Bestätigung oder Rückrufverfahren)

▶ **Social Engineering**
Social Engineering bezeichnet die Beeinflussung von Personen durch emotionale Manipulation mit dem Ziel, bestimmte Verhaltensweisen hervorzurufen – etwa die Preisgabe von vertraulichen Informationen oder zur Freigabe von Transaktionen.

▶ **Verhaltensanalyse (behavioural analytics)**
Durch die Analyse von Nutzerverhalten, wie z. B. Login-Zeiten, Standortwechsel oder Gerätewechsel, lassen sich Auffälligkeiten erkennen, die auf betrügerische Aktivitäten hinweisen. Diese Methode ergänzt technische Prüfmechanismen und erhöht die Reaktionsgeschwindigkeit bei verdächtigen Transaktionen.

Die FMA sieht einen weiteren Handlungsbedarf für Kreditinstitute in den folgenden Bereichen:

Verbesserung der Reaktionszeiten bei Betrugsmeldungen:
Bei Instituten ohne automatisierte Eskalationsprozesse sowie klaren Zuständigkeiten dauert es oft Stunden, bis Maßnahmen gegen einen gemeldeten Betrug ergriffen werden können. Ein kritischer Zeitraum, in dem oftmals noch Schadensbegrenzung möglich ist. Dieser Zeitraum sollte genutzt werden.

Weiterentwicklung von Transaktionsüberwachungssystemen:
Einige Institute verlassen sich noch immer auf starre Schwellenwerte (z. B. bei Überweisungshöhe oder Häufigkeit) und haben nur rudimentäre Parameter zur Erkennung von Betrugsszenarien etabliert, was zur Folge hat, dass neue Betrugsmuster lange unerkannt blieben. Eine laufende und rasche Anpassung von Betrugsszenarien zur Prävention ist unerlässlich.

Verbesserung der IT-Sicherheit:
IT-Governance und IT-Sicherheitsmaßnahmen sind auch im Bereich Zahlungsverkehr ein wichtiger Faktor, wenn es um Betrugsprävention geht, da Sicherheitslücken beim Zahlungsprozess zu erfolgreichen Betrugsversuchen führen können.

Regelmäßige Kontrolle der Sicherheitsmechanismen:
Eine regelmäßige Testung und Überprüfung durch interne oder externe unabhängige Prüfer:innen der etablierten Sicherheitsmechanismen insbesondere der Transaktionsüberwachung ist für die Gewährleistung wirksamer Maßnahmen zur Erkennung ständig ändernder Betrugsmethoden wichtig. Das Intervall einer externen Prüfung sollte je nach Ausgestaltung des Geschäftsmodells proportional gewählt werden.

Förderung der interinstitutionellen Zusammenarbeit
Eine Förderung der interinstitutionellen Zusammenarbeit ist wichtig. Beispielsweise für die Verhinderung von Betrug über betrügerisch erlangte eSIM-Karten ist ein regelmäßiger und transparenter Informationsaustausch zwischen Banken, Telekommunikationsprovider und Regulierungsstellen essenziell, um neue Betrugsmuster rasch zu erkennen und gemeinsam wirksame Gegenmaßnahmen zu entwickeln.

Ausblick und Fazit

Die Vermeidung vom Betrug im Zahlungsverkehr durch Kreditinstitute hat mit Sensibilisierungsmaßnahmen für die Verbraucher:innen Hand in Hand zu gehen. Für die Rolle und Verantwortung der Kreditinstitute zeigen die Ergebnisse der Marktanalyse, dass eine datenbasierte, kooperative Vorgehensweise und die konsequente Umsetzung bewährter Praktiken einen nachhaltigen Beitrag zur Reduktion von Betrugsrisiken leisten. Gleichzeitig macht der dynamische Wandel im digitalen Zahlungsverkehr deutlich, dass Sicherheitsmaßnahmen kontinuierlich angepasst und weiterentwickelt werden müssen.
Die FMA führt den Prüfschwerpunkt »Vermeidung von Betrug im Zahlungsverkehr« fort und wird dabei insbesondere

die Umsetzung der identifizierten Good Practices sowie die Behebung zentraler Schwachstellen in den Fokus rücken. Gleichzeitig sollen die gewonnenen Erkenntnisse zur Weiterentwicklung von Mindeststandards und zur Stärkung des aufsichtsrechtlichen Dialogs mit den beaufsichtigten Instituten beitragen.
Mit Blick auf die bevorstehende Umsetzung der Payment Services Directive (PSD3) und der neuen Payment Services Regulation (PSR) ist zudem davon auszugehen, dass die Anforderungen an Betrugsprävention und Transparenz weiter steigen werden. Mit der PSD2 wurde die starke Kundenauthentifizierung als verbindlicher Standard etabliert. Die PSD3 wird diesen Schutzrahmen weiter ausbauen, um aktuellen und künftigen Bedrohungsszenarien im digitalen Zahlungsverkehr zu begegnen. Zudem legt die PSD3 einen besonderen Fokus auf Verbraucherschutz. Künftig wird von Instituten ein höheres Maß an Verantwortung erwartet, um Betrugsrisiken wirksam zu adressieren und Verbraucher:innen proaktiv zu schützen. Die geplanten Neuerungen im Rahmen des neuen Regimes umfassen u. a. erweiterte Meldepflichten für Betrugsversuche, verpflichtende Rückerstattungsregeln bei bestimmten Betrugsarten sowie eine engere Zusammenarbeit zwischen Zahlungsdienstleistern und Telekommunikationsanbietern. Für Institute bedeutet das, sich frühzeitig mit den erwarteten Anforderungen vertraut zu machen und bestehende Präventionsmaßnahmen entsprechend weiterzuentwickeln.

▸ PSD 2
Payment Services Directive
Mit der Payment Service Directive 2 wurde starke Kundenauthentifizierung (SCA) und die Öffnung des Marktes für neue Anbieter eingeführt.

▸ PSD 3
Payment Services Directive
Eine weitere Überarbeitung ist in Planung, um Verbraucherschutz, Wettbewerb und Sicherheit zu verbessern.

▸ PSR
Payment Services Regulation
Die geplante direkt anwendbare Payment Services Regulation soll den einheitlichen Zahlungsverkehr neu gestalten und Open Banking, Transparenz und Verbraucherschutz vorantreiben.

Link

Die FMA informiert mit dem Format **»Reden wir über Geld«** über gängige Betrugsmaschen und den sicheren Umgang mit Geld.
www.redenwiruebergeld.fma.gv.at

Das **Finanz-ABC** der FMA erklärt zentrale Finanzbegriffe leicht verständlich und unterstützt damit die Aufklärung und Orientierung von Verbraucher:innen.
www.fma.gv.at → Finanz-ABC → Konto

Weitere Informationen zur **Conduct- und IT-Risikoaufsicht:**
www.fma.gv.at → Banken
→ Conduct- und IT-Risikoaufsicht über Banken

§ Wir stützen unsere Aussagen auf teils komplexe rechtliche Vorgaben, die wir am Rand ausweisen, oder leiten sie davon ab, ohne neues Recht zu schaffen, so dass über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten hieraus nicht abgeleitet werden können. Wir formulieren klare Erwartungshaltungen, die sich weitestmöglich auf Rechtsprechung und europäische Auslegungshilfen stützen, i. Ü. aber unsere eigene fachkundige Rechtsauffassung wiedergeben. Wir gehen mit der Zeit, weswegen wir uns die Aktualisierung der angeführten Orientierungshilfen jederzeit vorbehalten.
Obige Aufzählungen stellen keine abschließende Liste dar und sind jedenfalls nur ergänzend und klarstellend zu betrachten.