Finanzgruppe
Deutscher Sparkassen- und Giroverband

FOKUSPAPIER

Cyberkriminalität steigt stark an – Prävention erfordert koordiniertes Vorgehen in Europa

Cyberkriminelle gefährden Sicherheit und Vertrauen im digitalen Zahlungsverkehr. Die Zahlungsdiensteverordnung PSR-E wendet diese Bedrohung nicht ab. Nur verbesserte rechtlich-technische Koordination in ganz Europa kann massenhaften Betrug präventiv verhindern. Hier brauchen mündige Verbraucher sowie deren Banken und Sparkassen die Unterstützung der Politik.

Die Sparkassen-Finanzgruppe fordert von der deutschen und der europäischen Politik:

- Eine deutsche und europäische Verbraucherschutzpolitik, die Aufklärung, Eigenverantwortung und koordinierte Prävention gegen Cybercrime fördert
- Keine Fehlanreize durch pauschale Erstattungspflichten bei Social-Engineering-Betrug, bei dem korrekt autorisierte Zahlungen auf extern verursachter Täuschung beruhen.

Der digitale Zahlungsverkehr ist längst bevorzugtes Ziel organisierter Kriminalität. Social Engineering, Phishing-Webseiten, betrügerische Anrufe und Identitätsdiebstahl führten im Jahr 2024 laut Bundeskriminalamt (BKA) allein in Deutschland zu einem wirtschaftlichen Schaden von 1,7 Mrd. Euro. Mehr als 80 Prozent der Betrugsversuche im Zahlungsverkehr basieren auf Datendiebstahl, Telefonbetrug und manipulierten Netzwerken außerhalb der Bankensysteme. Laut BKA und Branchenanalysen ist das ein Anstieg der gemeldeten Fälle um mehr als 50 Prozent seit 2018.

Fehlanreiz durch Erstattungspflicht

Die geplante EU-Zahlungsdiensteverordnung (PSR-E) sieht lediglich eine pauschale Beweislastumkehr zulasten von Zahlungsdienstleistern vor. Doch das würde die Öffentlichkeit nur in falscher Sicherheit wiegen. Das Risikobewusstsein von Nutzerinnen und Nutzern würde geschwächt, wenn die Verantwortung alleinig den Finanzdienstleistern zugeschoben würde. Denn der Betrug findet auf gefälschten Webseiten und mithilfe betrügerischer Anrufe oder Nachrichten statt. Zahlungsdienstleister haben damit nichts zu tun, es liegt außerhalb ihres Verantwortungs- und Einflussbereichs. Die Getäuschten autorisieren Zahlungen eigenständig, technisch korrekt und gemäß regulatorischer Anforderungen. Eine automatische Erstattungspflicht würde vor allem Fehlanreize schaffen, Betrugsaktivitäten steigern und die Anfälligkeit des Gesamtsystems nur weiter erhöhen.

Pflichten auch für Technikanbieter

Die Täuschungen finden zwar mithilfe digitaler Technik statt, aber die Betreiber und Anbieter technischer Infrastrukturen sind heute kaum in die Bekämpfung von Internetkriminalität eingebunden. Eine wirksame Betrugsprävention kann nur gelingen, wenn der Gesetzgeber diese Akteure zu Präventionsmaßnahmen verpflichtet:

→ Telekommunikationsanbieter
→ Hosting-Provider
→ Soziale Netzwerke

Anbieter von Telekommunikation sollten auch hierzulande ein Verbot von Call-ID-Spoofing umsetzen, also die Anzeige falscher Telefonnummern im Display verhindern. Betreiber von Online-Plattformen und sozialen Netzwerken müssten betrügerische Telefonate identifizieren und schnell in der Lage sein, manipulative Inhalte und gefälschte Massen-Mailings zu erkennen und durch Löschung unschädlich zu machen.

Der Aufbau eines gemeinsamen europäischen Datenraums zur Betrugsbekämpfung (Fraud Sharing Hub) ist deshalb richtig. Diese Datenbank muss folgende Maßnahmen ermöglichen:

- Internationaler Austausch zwischen Polizei, Staatsanwaltschaft, Europol und Eurojust über Täterstrukturen und Zielkonten
- Früherkennung von neuen Betrugsmustern
- Rasche, sektorübergreifende Reaktion auf Bedrohungen.

„Eine automatische Erstattungspflicht würde vor allem Fehlanreize schaffen."

! Das fordert der DSGV:

→ **Verbraucherschutz durch geteilte Verantwortung statt pauschaler Beweislastumkehr**
→ **Europäische Koordinierung statt nationaler Einzelstrategien**
→ **Einbindung digitaler Plattformen und Kommunikationsdienste sowie Aufbau eines Fraud Sharing Hubs**

Kontakt

Stabsstelle Politik
und Regierungsbeziehungen
E-Mail: politik@dsgv.de

dsgv.de @DSGV

Herausgeber: **Deutscher Sparkassen- und Giroverband (DSGV),** Kommunikation und Medien, Charlottenstraße 47, 10117 Berlin