Cyberresilienz und Betrugsbekämpfung stärken

Berlin, 1. September 2026

bankenverband

Wo stehen wir…?

Die Digitalisierung verändert Wirtschaft und Gesellschaft grundlegend. Sie eröffnet neue Chancen für Innovation und Wachstum. Zugleich nehmen Cyberbedrohungen zu und stellen Unternehmen, Staat sowie Verbraucherinnen und Verbraucher vor neue Anforderungen an Sicherheit und Widerstandsfähigkeit. Cyberresilienz gehört deshalb zu den zentralen strategischen Aufgaben Europas.

Künstliche Intelligenz wird für Angriffe wie für die Abwehr eingesetzt.

KI-Modelle der neuesten Generation wie „Claude Mythos“ des Unternehmens Anthropic erkennen Software-Schwachstellen automatisiert und können sie in kurzer Zeit ausnutzen. Damit sinken die Einstiegshürden für Angriffe deutlich. Gleichzeitig bleibt Unternehmen weniger Zeit, um zu reagieren. Die Cybersicherheit steht damit vor einem grundlegenden Wandel: KI macht Angriffe einfacher, kann aber auch die Abwehr deutlich stärken.

DORA erhöht die digitale Resilienz des Finanzsektors.

Vor diesem Hintergrund gewinnt der Digital Operational Resilience Act (DORA) weiter an Bedeutung. Der einheitliche Rechtsrahmen stärkt die digitale Resilienz des Finanzsektors und setzt europaweit klare Anforderungen. Finanzunternehmen müssen sich auf mögliche Störungen intensiver vorbereiten, Risiken aktiv steuern, Sicherheitsvorfälle schnell bewältigen und ihre Handlungsfähigkeit regelmäßig testen.

Technologische Abhängigkeiten sind ein Risikofaktor.

Gerade bei zentralen digitalen Infrastrukturen und Cloud-Diensten müssen Unternehmen Konzentrationsrisiken verringern und Schwachstellen früh erkennen. Dafür brauchen sie Strategien, die mehrere Anbieter ermöglichen, den Wechsel von Dienstleistern erleichtern und den Zugriff auf Daten jederzeit sichern.

Online-Betrug ist ein gesamtgesellschaftliches Problem.

Digitale Resilienz endet jedoch nicht bei der technischen Abwehr von Cyberangriffen. Sie umfasst auch den Schutz vor digitalem Betrug.

Kriminelle richten ihre Manipulationen und Angriffe immer häufiger direkt auf den Menschen (Social Engineering). Sie verschicken gefälschte E-Mails und Nachrichten, bauen täuschend echte Websites, geben sich als Bankmitarbeitende aus oder nutzen soziale Medien als Einfallstore. So versuchen sie, sensible Daten zu erbeuten und ihre Opfer zu Zahlungen an Kriminelle zu bewegen.

Die finanziellen Schäden sind beträchtlich. Nach Angaben der Europäischen Aufsichtsbehörde EBA sowie der Europäischen Zentralbank (EZB) belief sich das Volumen betrugsbehafteter Zahlungen im Jahr 2024 auf rund vier Milliarden Euro.

Die Schutzmaßnahmen der Banken verhindern bereits heute deutlich höhere Schäden. Banken entwickeln ihre Schutzmechanismen laufend weiter. Ein Beispiel ist die seit 2025 europaweit eingeführte Empfängerüberprüfung („Verification of Payee“). Sie hilft Kundinnen und Kunden, manipulierte oder falsche Empfängerdaten zu erkennen, bevor sie eine Überweisung auslösen.

Wohin wollen wir…?

Ein widerstandsfähiger Finanzsektor

Der Finanzsektor muss auch unter neuen Bedrohungsszenarien handlungsfähig und stabil bleiben. DORA setzt dafür bereits auf einen ganzheitlichen Ansatz. Denn Cyberrisiken entstehen heute entlang ganzer Wertschöpfungs- und Lieferketten. Deshalb müssen Banken, Cloud-Anbieter, Technologiepartner und andere zentrale Dienstleister gemeinsam in den Blick genommen werden. Der Fokus verschiebt sich: Nicht mehr nur einzelne Systeme zählen, sondern die Widerstandsfähigkeit des gesamten Finanzsystems.

Cybersicherheit als strategische Aufgabe

Unternehmen müssen Cyberresilienz fest in Geschäftsstrategie, Unternehmenssteuerung und Risikomanagement verankern. KI kann Angriffe schneller sichtbar machen, Auffälligkeiten rascher analysieren und Lücken automatisiert schließen. Schutzmaßnahmen müssen sich laufend an neue Methoden der Angreifer anpassen – und ihnen im besten Fall einen Schritt voraus sein.

Vorsorge und Verantwortung in Balance

Online-Betrug betrifft die gesamte Gesellschaft. Keine Branche kann ihn allein verhindern. Wirksame Prävention braucht klare Haftungsregeln, gute Aufklärung und ein abgestimmtes Vorgehen aller Beteiligten. Auch Verbraucherinnen und Verbraucher tragen Verantwortung: Sie müssen Warnungen ernst nehmen, Informationen nutzen und Zahlungsentscheidungen sorgfältig prüfen.

Online-Betrug lässt sich nur gemeinsam bekämpfen

Das neue EU-Recht zur Betrugsbekämpfung im Zahlungsverkehr (EU-Zahlungsdiensteverordnung) ist ein wichtiger Schritt. Die Umsetzung wird jedoch anspruchsvoll. Langfristig wirken die Maßnahmen nur, wenn Banken, Sicherheitsbehörden, Telekommunikationsunternehmen, Plattformbetreiber und Verbraucherorganisationen abgestimmt handeln.

Warum ist das relevant?

- Kriminalität im digitalen Raum verursacht mehr als finanzielle Schäden. Jeder erfolgreiche Angriff schwächt das Vertrauen in digitale Angebote und trifft damit nicht nur einzelne Unternehmen, sondern die gesamte digitale Wirtschaft. Cybersicherheit und gezielte Betrugsbekämpfung stärken deshalb Wettbewerbsfähigkeit und Standortqualität. Zugleich sichern sie Europas digitale Souveränität und werden damit zu einer politischen Gestaltungsaufgabe.
- Wir müssen Verbraucherinnen und Verbraucher besser vor Täuschungsversuchen schützen, Schäden reduzieren und sie im besten Fall gar nicht erst entstehen lassen.
- Dafür müssen Vorsorge, Eigenverantwortung, technologische Schutzmaßnahmen, wirksame Strafverfolgung und ein abgestimmtes Vorgehen über Branchen- und Ländergrenzen hinweg ineinandergreifen.

Notwendige Maßnahmen

Ziel: Cyberresilienz erhöhen

Cyberresilienz braucht klare Regeln, technologische Vielfalt und einen starken Schulterschluss.

1 Cybersicherheit als gemeinsame Aufgabe von Staat, Wirtschaft und Aufsicht verankern

- Cyberangriffe treffen nicht nur einzelne Institute. Sie können die Stabilität des Finanzsystems, der Wirtschaft und der Gesellschaft insgesamt gefährden. Staat, Aufsicht und Finanzwirtschaft müssen Bedrohungen deshalb früh erkennen und entschlossen handeln.

2 Digitale Souveränität: Abhängigkeiten bewerten, technologische Vielfalt erhalten

- Digitale Resilienz verlangt auch einen sicheren Umgang mit externen Technologiepartnern. Banken müssen Dienstleister regelmäßig auf Schwachstellen prüfen. Zugleich brauchen sie die Freiheit, Lösungen zu wählen, die zu ihrem Geschäftsmodell sowie zu ihren Sicherheits- und Resilienzanforderungen passen. So lassen sich Gefahren begrenzen, Stabilität erhöhen und Innovation sowie Flexibilität erhalten.
- Genau daran sollte sich auch der derzeit auf europäischer Ebene entwickelte Cloud and AI Development Act orientieren. Wenn Regulierung die Auswahl auf wenige vermeintlich „souveräne“ Anbieter beschränkt, entstehen neue Abhängigkeiten – und damit neue Risiken für die Resilienz.

3 KI verantwortungsvoll einsetzen

- Banken setzen KI gezielt ein, um verdächtige Vorgänge, Anomalien und Cyberangriffe schneller zu erkennen. Ihre Abwehr muss mit den Fähigkeiten potenzieller Angreifer Schritt halten.

Betrugsbekämpfung gelingt nur mit Aufklärung, Technik und konsequentem Informationsaustausch.

Ziel: Betrugsbekämpfung wirksamer machen

1 Betrugsschutz als gesamtgesellschaftliche Aufgabe begreifen

- Die EU-Zahlungsdiensteverordnung (Payment Services Regulation, PSR) tritt ab 2028 in Kraft. Sie erweitert die Instrumente gegen Missbrauch, stärkt den Schutz von Kundinnen und Kunden und schafft neue Möglichkeiten, betrügerische Zahlungen zu erkennen und zu stoppen.

2 Verbraucheraufklärung und Eigenverantwortung fördern

- Kundinnen und Kunden müssen aktuelle Betrugsmaschen kennen und Risiken einschätzen können. Sicherheitsinstrumente wie die Empfängerüberprüfung („Verification of Payee") helfen dabei. Sie ersetzen aber nicht die Aufmerksamkeit bei Zahlungsentscheidungen. Wirksamer Schutz vor Online-Betrug verbindet Technik, finanzielle Bildung und Aufklärung.

3 Informationsaustausch zwischen Banken und anderen Branchen verbessern

- Cyberkriminelle handeln vernetzt und grenzüberschreitend. Banken brauchen deshalb rechtssichere Wege, um betrugsrelevante Informationen untereinander sowie mit Telekommunikationsunternehmen und Behörden auszutauschen.

4 Spoofing unterbinden

- Kriminelle missbrauchen manipulierte Rufnummern und täuschen Anrufe oder Nachrichten von Banken, Behörden oder anderen vertrauenswürdigen Institutionen vor. Dieses sogenannte Spoofing treibt Betrug im digitalen Raum und schwächt das Vertrauen in digitale Kommunikation. Telekommunikationsanbieter sollten deshalb technische Maßnahmen zur Authentifizierung und Validierung von Rufnummern flächendeckend umsetzen. Sie müssen gefälschte Absenderrufnummern verhindern und bekannte betrügerische Nummern schneller blockieren.
- Auch der Gesetzgeber muss handeln: Er muss die rechtlichen Voraussetzungen schaffen, damit Telekommunikationsanbieter solche Maßnahmen rechtssicher, wirksam und flächendeckend umsetzen können. Nur so lässt sich Betrug wirksam vorbeugen.

Herausgeber:
Bundesverband deutscher Banken e. V.

Burgstraße 28
10178 Berlin
Deutschland

Lobbyregister-Nr. R001458
EU-Transparenzregister-Nr. 0764199368-97
USt-IdNr.: DE201591882

Kontakt:
bankenverband@bdb.de
+49 30 1663-0
bankenverband.de

Inhaltlich verantwortlich:
Themengruppe Banktechnologie und Sicherheit sowie Zahlungsverkehr
André Nash, Leiter Banktechnologie und Sicherheit
Dr. Ingo Beyritz, Leiter Zahlungsverkehr

bankenverband