KI, Open Banking und die wachsende Cyber-Bedrohung

Sicherheit stärken, damit Finanzinstitute die Oberhand behalten

Die Cyberkriminalität blüht, und der Finanzsektor ist ein bevorzugtes Ziel.

Angreifer skalieren ihre Operationen mit KI und nutzen Schwachstellen in APIs, offenen Bankstandards und Systemen von Drittanbietern aus. In diesem Umfeld kann ein schwaches Glied ein ganzes System gefährden – und so werden aus ehemals nebensächlichen IT-Problemen geschäftskritische Bedrohungen.

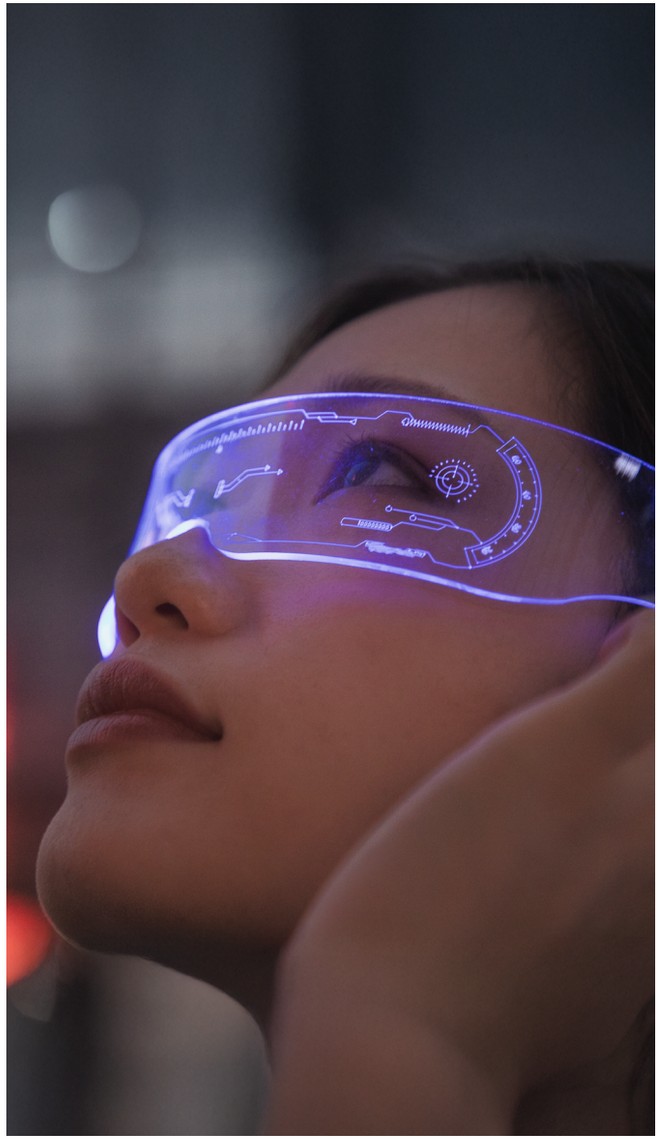
Und das ist noch nicht alles. Kriminelle Netzwerke sind heute organisiert, finanziert und effizient. Sie operieren wie Unternehmen und nutzen Kosten-Nutzen-Modelle, Investitionsstrategien und ausgefeilte Taktiken, um ihren Gewinn zu maximieren.

> Cyberkriminalität wird zum Business Case: Die Investition muss sich lohnen
>
> Lars Weimer
> EY

Mit zunehmendem Umfang und zunehmender Komplexität werden Angriffe immer schwieriger vorherzusagen – und noch schwieriger einzudämmen.

Aus diesem Grund muss Cybersicherheit eine strategische Priorität sein.

Denn mit den Kriminellen entwickeln sich auch ihre Werkzeuge weiter – und KI ist ihre schärfste Waffe.



Der neue Konflikt: KI und Sicherheit

KI ist ein zweischneidiges Schwert. Sie hilft Verteidigern, Bedrohungen schneller zu erkennen. Aber sie ermöglicht es auch Angreifern, ihre Attacken zu automatisieren, zu personalisieren und zu skalieren.

87%

der Entscheidungsträger im Bereich Betrug sagen, dass ihre Bank durch KI schneller auf Bedrohungen reagieren kann.[1]

69%

glauben, dass Kriminelle bei der Nutzung von KI weiter fortgeschritten sind als Banken.[2]

Da Cyberkriminelle immer raffinierter werden, müssen Finanzinstitute KI zur Verteidigung nutzen und gleichzeitig vorhersehen, wie sie als Waffe eingesetzt werden könnte. Zumal die zunehmende Konnektivität über verschiedene Systeme hinweg das Risiko vervielfacht – was durch Open Banking noch weiter in den Vordergrund gerückt wird.

Die Chancen

- Schnellere Erkennung und Prävention von Bedrohungen
- Lernt aus Nutzerverhalten, um Attacken zu antizipieren
- Warnt vor Anomalien und Mustern in Echtzeit
- Ermöglicht automatisierte Reaktions-maßnahmen

Die Bedrohungen

- Verbessert Malware, um Entdeckung zu vermeiden
- Ermöglicht Phishing-Attacksen im großen Stil
- Optimiert Attacken für maximale Wirkung
- Vertieft Social Engineering

[1] BioCatch. AI, Fraud and Financial Crime Survey. 2024. Online survey of 600 fraud management experts at banks across EMEA, APAC, and North America. https://www.biocatch.com/ai-fraud-financial-crime-survey (Accessed 24, April 2024)

[2] BioCatch. AI, Fraud and Financial Crime Survey. 2024. Online survey of 600 fraud management experts at banks across EMEA, APAC, and North America. https://www.biocatch.com/ai-fraud-financial-crime-survey (Accessed 24, April 2024)

Open Banking: mehr Innovation, mehr Angriffsfläche

Während Open Banking bessere Nutzererfahrungen und Auswahlmöglichkeiten schafft, kann es auch zu einer Fragmentierung führen. Unterschiedliche Standards und Annahmen machen es Kriminellen leichter, Lücken zu finden. APIs und Verbindungen von Drittanbietern mit unzuverlässigem Schutz bedeuten, dass eine einzige anfällige Verbindung die gesamte Kette gefährden kann.

> Open Banking ist ein riesiger Bereich, der Lücken schafft, die Angreifer ausnutzen.
>
> Lars Weimer
> EY

Schlüsselrisiken für die Sicherheit:

Falsch konfigurierte oder ungesicherte APIs

Eine einzige Schwachstelle kann ganze Systeme angreifbar machen.

Lücken bei Drittparteien

Inkonsistente Partnerstandards schaffen Schwachstellen.

Schwache Zugangskontrollen

Unzureichende Kontrollen können unbefugten Zugriff erleichtern.

Phishing und Social Engineering

Gefälschte Websites und E-Mails verleiten zur Weitergabe von Daten.

Störung der Abläufe

Angriffe oder Ausfälle können Prozesse stören – und Vertrauen.

Sicherheitsmaßnahmen sind keine einmalige Investition

Man muss bedenken, dass Sicherheit nicht statisch ist. Die Schutzmaßnahmen müssen sich entsprechend den neuen Bedrohungen weiterentwickeln. Dazu braucht es mehr als nur Technik, sondern auch die richtige Denkweise, Strategie und Kultur.

Echte Widerstandsfähigkeit entsteht durch die Kombination robuster Systeme mit einer Kultur, in der die erste Sicherheitsmaßnahme Menschen sind.

Um Risiken zu mindern und Kriminellen zuvorzukommen, müssen sich Institutionen auf Folgendes konzentrieren:

Kontinuierliche Sicherheitstests

Mit regelmäßigen Tests Schwachstellen entdecken, bevor es Kriminelle tun.

Risikomanagement bei Drittparteien

Vertraute Partner suchen und diese oft evaluieren, um Compliance sicherzustellen.

Vorbereitung bei Vorfällen

Ein guter Plan antizipiert Angriffe, reduziert ihre Wirkung und beschleunigt die Wiederherstellung der Sicherheit.

Steuerung und Transparenz

Definierte Verantwortlichkeiten, Übersicht und Echtzeitreporting verbessern die Sicherheit.

Menschen: Ihre stärkste Verteidigung

Wie fortschrittlich die Technologie auch sein mag, Angreifer werden es immer auf Menschen abgesehen haben, die unaufmerksam sind."

Lars Weimer
EY

Menschliche Aufmerksamkeit ist nach wie vor eine der besten Verteidigungsmaßnahmen gegen Cyber-Bedrohungen. Aber sie kommt nicht von nichts. Sie wird gewährleistet durch Beständigkeit, Führung und fortlaufende Schulungen, die zur Gewohnheit werden. Vor allem aber geht es bei einer widerstandsfähigen Sicherheitskultur um gemeinsame Verantwortung auf allen Ebenen.

88%

der Betrugsexperten wünschen sich innerhalb von zwei Jahren einen stärkeren Datenaustausch zwischen Banken, Finanzinstituten und Aufsichtsbehörden, um die Finanzkriminalität zu bekämpfen.[3]

Eine sicherheitsfokussierte Kultur aufbauen

Einbindung der Mitarbeiter:innen

Ermutigung zur aktiven Beteiligung in der gesamten Organisation. Ermächtigen Sie die Mitarbeiter:innen, ihre Meinung zu äußern, zu hinterfragen und Bedenken zu melden.

Akzeptanz auf Vorstandsebene

Wenn die Führungsebene Cybersicherheit ernst nimmt, folgt das Unternehmen diesem Beispiel. Machen Sie es zu einer strategischen Priorität.

Branchenübergreifende Zusammenarbeit

Austausch von Informationen und bewährten Verfahren. Die Widerstandsfähigkeit verbessert sich, wenn Institutionen ihre Silos aufbrechen und zusammenarbeiten.

Cybercrime wird nicht langsamer, aber Ihre Verteidigung kann schneller werden.

Visa arbeitet mit führenden Finanzdienstleistern zusammen, um die Widerstandsfähigkeit zu erhöhen, Risiken zu verringern und die Reaktion der Branche auf sich entwickelnde Bedrohungen zu stärken. Die Frage ist nicht, ob Bedrohungen auftreten werden, sondern wie gut Sie darauf vorbereitet sind, zu reagieren, sich zu erholen und sich anzupassen.

Möchten Sie mehr erfahren?

Setzen Sie sich mit uns in Verbindung, um zu erfahren, wie wir Unternehmen dabei helfen, den Bedrohungen einen Schritt voraus zu sein.

Kontaktieren Sie uns ›

[3] BioCatch. AI, Fraud and Financial Crime Survey. 2024. Online survey of 600 fraud management experts at banks across EMEA, APAC, and North America. https://www.biocatch.com/ai-fraud-financial-crime-survey (Accessed 24, April 2024)

