FIRM
Frankfurter Institut für Risikomanagement und Regulierung

KI-Rüstung: Schutz von Banken mit fortschrittlicher vernetzter Analytik

In der heutigen globalen, vernetzten Welt bleibt das Risiko der Wirtschaftskriminalität eine allgegenwärtige Herausforderung. Regulatoren auf der ganzen Welt signalisieren ihre steigenden Erwartungen, dass die Compliance-Programme immer zielgerichteter werden. Die Art und Weise, wie sich Finanzinstitute gegen Risiken wie Betrug, Geldwäsche, Terrorismusfinanzierung und Cyberangriffe schützen, hat sich durch den Einsatz von künstlicher Intelligenz (KI), insbesondere durch fortschrittliche vernetzte Analysen, erheblich verändert. Dieser Artikel fasst zusammen, wie KI die Sicherheit im Bankwesen (und gleichzeitig die Kosteneffizienz) erhöht, zeigt einen konkreten Anwendungsfall und analysiert die Auswirkungen auf die Branche.

DIE NOTWENDIGKEIT VON KI FÜR DIE BANKENSICHERHEIT

Der Finanzsektor ist nach wie vor ein Hauptziel für kriminelle Aktivitäten, da die Banken mit immer raffinierteren Bedrohungen konfrontiert sind, die durch die ständig wachsende und sich entwickelnde Handelsbeziehungen noch verschärft werden. Die Verbreitung neuer Zahlungssysteme und die Nachfrage nach schnelleren Zahlungen bedeuten zum Beispiel, dass die Banken immer weniger Zeit haben, ungewöhnliche Transaktionen zu erkennen. Gleichzeitig können Large-Language-Models und KI-Anwendungen in den falschen Händen Betrug begünstigen, indem sie Betrügern beispielsweise helfen, traditionelle Authentifizierungsmechanismen zu umgehen. Herkömmliche Kontrollmaßnahmen sind zwar nach wie vor unerlässlich, reichen aber oft nicht aus, um der Dynamik moderner Wirtschaftskriminalität zu begegnen. Diese Realität erfordert einen proaktiveren und intelligenteren Ansatz zur Erkennung und Vorbeugung von Bedrohungen, bei dem die Daten, die die Banken in Bezug auf Geschäftspartner, Geräte, Verhaltensweisen, Transaktionen und Netzwerke besitzen, stärker genutzt werden. KI, insbesondere fortschrittliche vernetzte Analytik, bietet eine leistungsstarke Lösung, da sie es den Banken ermöglicht, riesige Datenmengen aus verschiedenen Quellen in Echtzeit zu verbinden und zu analysieren. Diese Fähigkeit ermöglicht es Instituten, Anomalien zu erkennen, potenzielle Bedrohungen zu identifizieren und schnell auf inhärente Risiken zu reagieren. Fortschrittliche vernetzte

Analytik ermöglicht es Banken, Rohdaten in verwertbare Erkenntnisse über Kunden und verbundene Parteien, Zahlungen und Überweisungen, Produkte und Technologie umzuwandeln – all dies, um Vermögenswerte zu schützen und das Vertrauen der Kunden zu erhalten.

ERWEITERTE VERNETZTE ANALYTIK: EINE NEUE ÄRA DER SICHERHEIT

Bei der vernetzten Analyse geht es darum, unterschiedliche Datenquellen zu integrieren, um einen viel besseren Überblick über potenzielle Bedrohungen zu erhalten. Im Bankkontext bedeutet dies, dass Informationen aus statischen Daten, Transaktionsdaten, Kundeninteraktionen, sozialen Medien und externen Bedrohungsdatenquellen zusammengeführt werden. KI-Algorithmen, wie z.B. Machine-Learning, Entity Resolution und Netzwerkanalyse, spielen eine entscheidende Rolle bei der Analyse und Interpretation dieser Daten. Diese fortschrittlichen vernetzten Analysemodelle können komplexere und ausgefeiltere Muster erkennen, die auf potenziell betrügerisches Verhalten hindeuten und über die traditionellen Indikatoren wie ungewöhnliche Transaktionsvolumina oder Abweichungen von typischen Ausgabengewohnheiten hinausgehen. Darüber hinaus können KI-Systeme kontinuierlich aus neuen Daten lernen und sich anpassen und so ihre Vorhersagekraft im Laufe der Zeit verbessern. Diese Fähigkeit des dynamischen Lernens ist entscheidend, um den sich ständig weiterentwickelnden Strategien von Kriminellen auf kosteneffiziente Weise zu begegnen.

BEISPIEL AUS DER PRAXIS: KI-GESTÜTZTE ERKENNUNG VON GELDKURIEREN

Um gegen ausgeklügelte Finanzkriminalität vorzugehen, hat eine weltweit führende Bank erheblich in KI investiert, um ungewöhnliche Muster und Verhaltensweisen zu erkennen. Mithilfe von Machine-Learning hat die Bank mehrere Merkmale in Modelle integriert, die jeweils ein anderes Verhalten darstellen. Auf diese Weise konnte sie Muster erkennen, die mit Mule-Konten in Verbindung gebracht werden, die normalerweise auf der Grundlage einzelner Datenquelle nur sehr schwer zu erkennen sind. So reicht beispielsweise eine große Einzelzahlung im Verbindung mit dem Gesamtkontostand nicht aus, um Mule-Konten aufzuspüren. Aber durch die Kombination verschiedener Indikatoren, wie z.B. eine kürzlich erfolgte Adressänderung, das Hinzufügen neuer Telefonnummern zur Authentifizierung, Transaktionen an mehrere neue Empfänger, ein sprunghafter Anstieg der Geldeingänge usw.,

und auf der Grundlage einer differenzierteren Analyse konnte die Bank wirklich verdächtige Aktivitäten genauer identifizieren und Risiken erkennen. Die Bank entdeckte auch, dass ein Ansatz, der auf einer kontinuierlichen Entwicklung basiert, am besten funktionierte, und sie war in der Lage, Daten in Modelle einzuspeisen, um im Laufe der Zeit genauere Vorhersagen zu treffen. Mithilfe dieser Modelle, die auf fortschrittlicher, vernetzter Analytik basieren, konnte die Bank dreimal mehr Mule-Konten aufdecken als zuvor.

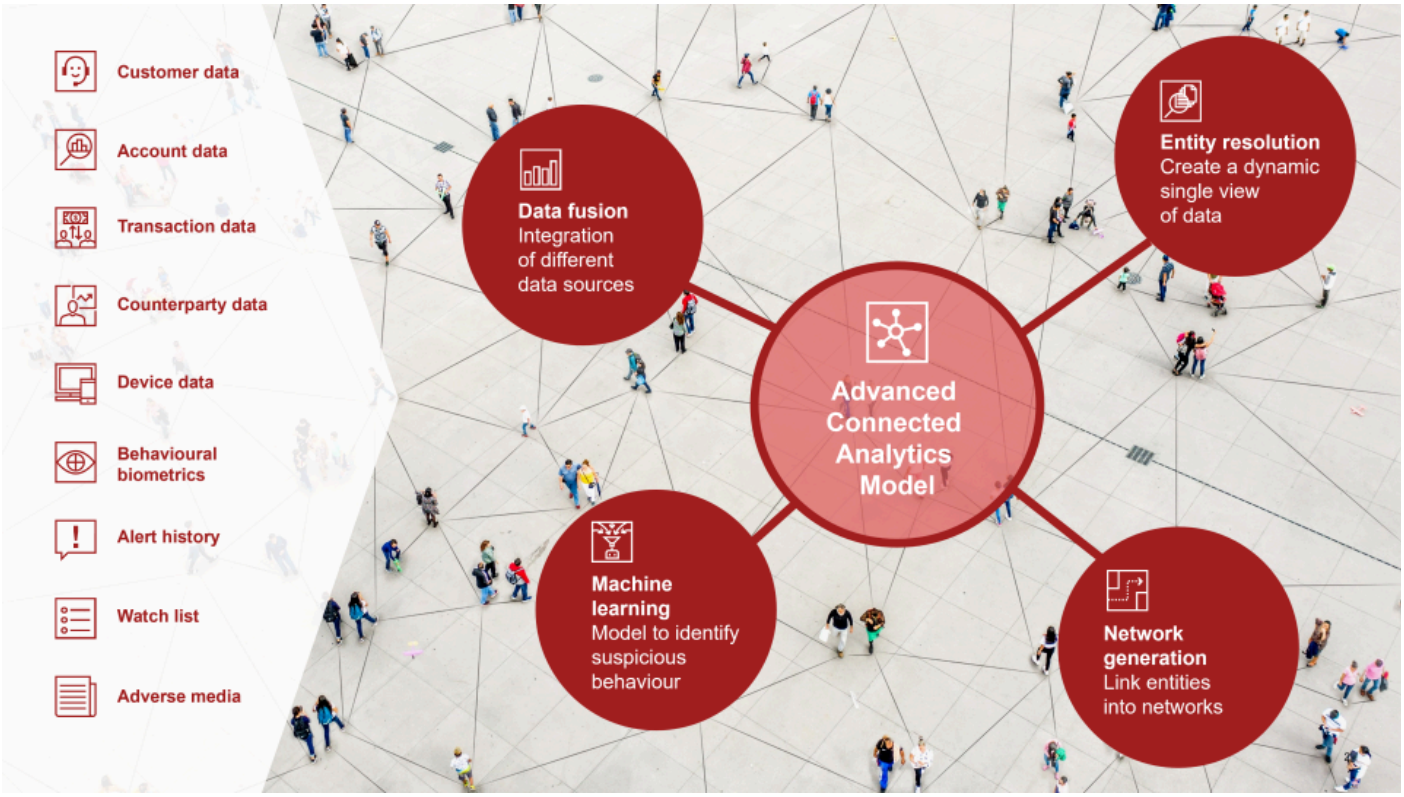

Abbildung 1: Fortgeschrittene, vernetzte Analytik zur Identifizierung von Mule-Konten

IMPLIKATIONEN UND ZUKÜNFTIGE WEGE

Die Einbeziehung von KI in die Sicherheit hat verschiedene Auswirkungen auf den Bankensektor. Zunächst einmal wird deutlich, wie wichtig es für Banken ist, in Spitzentechnologie und Dateninfrastruktur zu investieren. Das Kaliber und die Vielfalt der Daten, auf die KI-Systeme zugreifen können, bestimmen, wie effektiv sie sind. Um das Potenzial von KI effektiv nutzen zu können, müssen Banken der Datenintegration und -management höchste Priorität einräumen. Zweitens erfordert die Implementierung von KI in der Bankensicherheit einen Wandel in der Unternehmenskultur und im Fachwissen.

Finanzinstitute müssen über Mitarbeiter verfügen, die sich mit KI und Data Science auskennen sowie komplexe Analysemodelle erstellen und beaufsichtigen können. Um Sicherheitsprobleme zu lösen, müssen die Banken auch eine innovative und kooperative Kultur fördern, die interdisziplinäre Teams zur Zusammenarbeit ermutigt.

Die Zukunft der KI in der Bankensicherheit ist eine Selbstverständlichkeit. Technologische Entwicklungen wie Deep Learning und Natural-Language-Processing haben das Potenzial, die Erkennung von Bedrohungen noch weiter zu verbessern. Durch die Analyse unstrukturierter Daten, einschließlich E-Mails und Social-Media-Posts, können diese Technologien den Banken ein besseres Verständnis für mögliche Risiken vermitteln. Darüber hinaus birgt die KI in der Bankensicherheit sowohl Potenzial als auch Herausforderungen, die sich aus der Entwicklung des Quantencomputings ergeben. Obwohl das Quantencomputing in der Lage ist, bestehende Verschlüsselungstechniken zu knacken, bietet es auch die Möglichkeit, effektivere KI-Algorithmen zu entwickeln, die große, komplizierte Datensätze mit bisher ungekannter Geschwindigkeit und Genauigkeit verarbeiten können.

FAZIT

KI-gestützte vernetzte Analytik ist ein leistungsstarkes Werkzeug im Arsenal moderner Banken, die sich vor kriminellen Handlungen schützen wollen. Durch den Einsatz von KI können Finanzinstitute Bedrohungen besser erkennen und verhindern, ihre Ressourcen schützen und das Vertrauen ihrer Kunden erhalten. Die Einbindung von KI in die Bankensicherheit wird zweifellos eine neue Ära des intelligenten Schutzes in der Finanzdienstleistungsbranche einleiten, die mit der Entwicklung des Finanzumfelds noch wichtiger wird.

QUELLEN

HSBC Holdings plc. „Annual Report and Accounts 2023.“ HSBC, 2023, Seite 45-47

Finanzstabilitätsrat. „Künstliche Intelligenz und maschinelles Lernen in Finanzdienstleistungen: Fortschrittsbericht.“ FSB, 2022, Seiten 10-15

Europäische Bankenaufsichtsbehörde. „Bericht über die Nutzung von Big Data und fortgeschrittenen Analysen im Bankensektor“. EBA, 2023, Seiten 22-30

PwC. Globale Umfrage zu Wirtschaftskriminalität und Betrug, 2024
https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Deloitte. „KI und Bankwesen: Mit der Zeit gehen". Deloitte Insights, 2023, Seiten 5-9

Accenture. „Das neue Zeitalter des Bankwesens: KI für den Wettbewerbsvorteil nutzen". Accenture, 2023,
Seiten 14-19

AUTOREN

Dominik Käfer

Partner/ Geschäftsführer,
European Head of Risk and Regulatory
strategy&

Dr. Lue Wu

Director, Risk and Regulatory
strategy&