Börsen-Zeitung
Zeitung für die Finanzmärkte

Ausgabe **68** vom **10.04.2021**, Seite 2

Via Deep Fake kann jeder Chef spielen

Gesichts- und Stimmen-Klone erleichtern Betrug – Aufsicht erwartet Auseinandersetzung mit diesem Risiko

Das virtuelle Klonen von Gesichtern und Stimmen wird alsbald ein Kinderspiel sein. Angesichts der rasanten technologischen Entwicklung und der Verfügbarkeit der erforderlichen Software – für Otto Normalverbraucher wie für Betrüger – sehen Fachleute Gefahren für Firmen und Kreditinstitute. Die EZB-Bankenaufsicht erwartet daher von der Kreditwirtschaft, dass sie sich näher mit dem neuen Risiko auseinandersetzt.

Von Tobias Fischer, Frankfurt

Börsen-Zeitung, 10.4.2021

Der Hochstapler, der sich als französischer Verteidigungsminister Jean-Yves Le Drian ausgibt, tritt mit maßgefertigter Silikonmaske in einem nachgebauten Ministerbüro vor die Kamera. Eine säuberlich drapierte Fahne und auch das Konterfei des zu der Zeit – wir schreiben das Jahr 2015 – amtierenden Staatspräsidenten François Hollande fehlen nicht. Die Bildqualität auf Skype lässt zwar zu wünschen übrig, aber alles in allem wirkt der filmreife Fake auf das ein oder andere Opfer glaubwürdig.

Ein Gefallen fürs Vaterland

Insgesamt 80 Mill. Euro soll eine israelisch-französische Bande über Jahre ergaunert haben – mal so, via Video, mal per Telefon, mal schriftlich. Der vermeintliche Minister und seine beiden Komplizen baten von 2015 an schwerreiche Geschäftsleute, aber auch Politiker, Diplomaten und Geistliche um einen Gefallen fürs französische Vaterland: Mit den Geldern sollten angeblich Geiseln aus der Gefangenschaft von Terroristen freigekauft werden, unter strengster Geheimhaltung versteht sich. 2019 flog das Trio auf.

Was schon vor Jahren analog funktionierte, wird künftig dank digitaler Fälschungsmethoden noch viel einfacher und besser möglich sein. Deep Fakes, mit künstlicher Intelligenz (KI) fabrizierte Videos, Bilder und Tonaufnahmen, treiben seit wenigen Jahren im Internet ihr Unwesen. Kommen sie bisher überwiegend als Videos pornografischen Inhalts und in überschaubarer Qualität daher, so werden die Fälschungen immer hochwertiger und wecken das Interesse von Kriminellen, politischen Spindoktoren und Geheimdiensten.

Deep Fakes machten Schwindel wie im Falle des Le-Drian-Klons „beunruhigend einfach“, sagt Henry Ajder von der Technologiefirma Sensity. Er fürchtet, dass Cyberkriminelle aus öffentlich zugänglichen Fotos und Audiodateien „Puppen“ von Firmenchefs und anderen wichtigen Personen erstellen. Das früher unter dem Namen Deeptrace auftretende Start-up aus Amsterdam hat Methoden entwickelt, um die Fälschungen mit Hilfe von KI ausfindig zu machen.

Noch sind nur wenige Fälle bekannt, in denen Deep Fakes missbräuchlich verwendet wurden, um Geld zu ergaunern. An die Öffentlichkeit gedrungen ist der CEO-Schwindel, dem der Leiter der britischen Niederlassung eines deutschen Energiekonzerns vor zwei Jahren zum Opfer fiel. Er hatte einen Betrüger am Apparat, der Chef spielte. Mittels Stimmenimitationssoftware klang er täuschend echt und verleitete den Mann zur Überweisung von 220 000 Euro auf ein Konto in Ungarn. Das Geld war futsch.

Meldung an EZB nötig

Aus dem Finanzsektor ist Vergleichbares bislang nicht bekannt, was nicht heißen muss, dass nichts passiert ist. Die Finanzaufseher haben das Thema nach eigenem Bekunden jedenfalls als potenzielle Bedrohung auf dem Schirm und erwarten Selbiges von den Instituten, wie die EZB-Bankenaufsicht auf Nachfrage erklärt: „Cyberangriffe nehmen zu, vor allem mit wachsenden Online-Aktivitäten in der Pandemie. Dazu können Angriffe über Deep-Fake-Techniken gehören. Die EZB-Bankenaufsicht erwartet von den Banken, dass sie alle Risiken, denen sie ausgesetzt sind, bewerten und diese effektiv entschärfen.“ Auch zur Meldung etwaiger Attacken unter Zuhilfenahme von Deep Fakes seien die Institute verpflichtet, bekräftigt ein Sprecher: „Banken müssen signifikante Cybervorfälle an die EZB-Bankenaufsicht melden, sobald sie diese entdecken, unabhängig davon, welche Technik die Angreifer verwendet haben.“

Als unheilvolle Einsatzgebiete für Deep Fakes sei – erst recht in Zeiten erschöpfender Remote-Arbeit – so ziemlich alles denkbar, sagt Digitalexpertin Agnieszka Walorska von der Management- und Technologieberatung Capco. „Der Kreativität sind keine Grenzen gesetzt.“ So bestehe die Gefahr, dass sich Identitätsprüfungen bei Kontoeröffnungen etwa in Verbindung mit einem gestohlenen Ausweis austricksen

Deep Fakes in Kürze

- Deep Fakes sind mit Hilfe von künstlicher Intelligenz (KI) hergestellte Videos, Audio- oder Bildformate. Die Resultate sind bisweilen täuschend echt wirkende synthetische Gesichts- oder Sprachimitationen.
- Deep Fake ist ein Kunstwort aus Deep, was für Deep Learning steht, und Fake. Deep Learning ist eine Form der Informationsverarbeitung und ein Teilsektor des maschinellen Lernens, bei dem eine Maschine selbständig lernt, ohne weiteres menschliches Zutun.
- Deep Learning nutzt neuronale Netze zur Analyse von Datenbergen. Nach Angaben von Microsoft handelt es sich dabei teils um dem neuronalen Netz nachempfundene Prozesse, welche das menschliche Gehirn verwendet.
- Um Deep Fakes zu erstellen, werden die künstlichen neuronalen Netze mit Fotos oder Tonaufnahmen einer bestimmten Person „gefüttert“.
- Im Unterschied zu den KI-fabrizierten Deep Fakes sind Cheap Fakes billige Fälschungen, indem etwa via herkömmliche digitale Bildbearbeitung ein Kopf auf einen anderen Körper gesetzt wird oder Filmaufnahmen langsamer oder schneller abgespult werden. Bekannt wurde ein Video der Sprecherin des US-Repräsentantenhauses, Nancy Pelosi, in dem sie eine Rede hält. Das Ganze ist echt, nur läuft das Video etwas langsamer, sodass Pelosi betrunken wirkt.

lassen. „Bisher heißt es, dass biometrische Verfahren in der Lage sind, Fälschungen zu entdecken“, sagt Walorska. „Aber auch sie müssen besser werden, weil Deep Fakes besser werden. Deshalb müssen wir in Zukunft mit solchen Betrugsfällen rechnen.“

Diese Befürchtung hegt auch Sensity-Forschungschef Ajder. Biometrische Sicherheitsmaßnahmen wie die Stimm- und Gesichtserkennung, die bei automatisierten Verfahren zur Identifizierung für das Onboarding von Bankkunden verwendet würden, könnten von Deep Fakes kompromittiert werden, „die diese Merkmale einer Person nahezu perfekt nachbilden können“.

Vorstellbar sind nach Ansicht von Capco etwa gefälschte Aussagen hochrangiger Bankmanager über Fusionen, über Verkäufe, über die finanzielle Lage des Unternehmens, die den Aktienmarkt beeinflussen. Oder dass wie im Fall des Energieunternehmens der vermeintliche Chef anruft, um einen Geldtransfer anzuweisen. Insbesondere Social Engineering, also dem Erschleichen von Vertrauen oder dem Ausüben von Druck, ist mit Deep Fakes Tür und Tor geöffnet. „Den Enkeltrick macht das um einiges einfacher“, sagt Walorska. „Man stelle sich vor, die scheinbare Bankberaterin ruft die Kundin an, die sie seit 30 Jahren kennt, und verlangt ein Passwort oder Ähnliches.“ Derlei Attacken lasse sich schwerlich vorbeugen.

Und auch im Nachhinein werde es diffizil, sagt ihre Kollegin Kathrin Meuthen, Cybersecurity-Expertin bei Capco. „Ich kann einen Einbruch so weit nachverfolgen, wie jemand Spuren hinterlassen hat. Aber was ist in einem solchen Fall zu tun?“ Aktuell seien Aufklärung und hohe Aufmerksamkeit die wichtigsten Gegenmaßnahmen gegen Deep Fakes.

Auch nutzten viele Unternehmen Whatsapp oder andere Messaging-Dienste, über die sich gefälschte Nachrichten verbreiten ließen, gibt Meuthen zu bedenken. Davor warnt auch Euler Hermes. Dem Kreditversicherer zufolge brachten Betrüger nach einem anfänglichen Telefonat einen Kfz-Zulieferer mittels nachfolgender Whatsapp-Textnachricht um 180 000 Euro und kassierten in einem anderen Fall 65 000 Euro.

Einsatz auch in Echtzeit

Mit rasant fortschreitender Technologie bietet sich die Gelegenheit, Deep Fakes in Echtzeit einzusetzen. Waren frühere Varianten statisch und mussten erst generiert werden, bevor sie zum Einsatz gelangen konnten, so sind mittlerweile realitätsnahe Live-Deep-Fakes möglich, mit denen jemand per Videochat mit dem Aussehen und der Stimme eines anderen kommunizieren kann. Die Technologie sei inzwischen so ausgefeilt, berichtet Walorska, dass zum Trainieren der KI nicht mehr wie früher massenweise Bild- und Videomaterial – etwa von Promis – nötig sei, sondern schon ein paar Fotos einer x-beliebigen Person genügten. Das gelte auch für Audio-Deep-Fakes, die lediglich mit wenigen Sätzen gefüttert werden müssten, um eine Stimme zu klonen.

Auch wenn das Phänomen Deep Fake bislang kein größeres Aufsehen im Geschäftsleben erregt hat, gehen Meuthen und Walorska davon aus, dass es nicht dabei bleibt. Zum einen sei von einer Dunkelziffer auszugehen, weil sich natürlich kein Unternehmen eingedenk des Reputationsschadens outen wolle, einem Deep-Fake-Schwindel auf den Leim gegangen zu sein. Zum anderen werde früher oder später ein spektakulärer Fall ans Licht kommen, der sich nicht verheimlichen lasse und das Bewusstsein für das Risiko schärfen werde, sind sie überzeugt. „Ich kann mir nicht vorstellen, dass diese Technologie, die immer besser wird, nicht im wirtschaftskriminellen Kontext genutzt wird“, sagt Walorska.

Es gebe aktuell simplere Möglichkeiten der Manipulation und des Betrugs, die sich in ihrer Effektivität KI-gestützten Vorgehensweisen als ebenbürtig erwiesen, befindet Vincenzo Ciancaglini von der japanischem IT-Sicherheitsfirma Trend Micro. „Man braucht diese ausgefeilten KI-Techniken im Moment nicht. Wir befinden uns noch an einem Punkt, an dem die einfache Fälschung von Dokumenten und Ähnlichem vergleichbare Resultate zeitigt“, sagte der Senior Threat Researcher jüngst bei einer Online-Veranstaltung zur missbräuchlichen Nutzung von KI durch Cybergangster.

Das werde sich aber sehr bald ändern. Er beobachte, dass manche Online-Kriminelle ihre Vorgehensweise zu modifizieren begännen und sie sich fortschrittlicherer Methoden wie KI bedienten. „Auch wenn ein groß angelegter Missbrauch von Deep Fakes durch böswillige Akteure und insbesondere Kriminelle bisher nicht zu beobachten war, ist es von Bedeutung, das Potenzial dieser Technologie in Verbindung mit der zunehmenden Zugänglichkeit und der steigenden Qualität von Tools zur Erstellung von Deep Fakes zu sehen“, heißt es in einem von Ciancaglini mitverfassten Forschungsbericht. Der von Trend Micro, der europäischen Polizeibehörde Europol und dem UN-Institut für Kriminalitätsforschung (Unicri) im November veröffentlichte Bericht konstatiert eine Zunahme manipulierter Bilder und Videos für kriminelle Zwecke.

Als mögliche Anwendungsgebiete identifizieren die Autoren gegen Politiker gerichtete Desinformationskampagnen, um das Vertrauen in Wahlen und die Demokratie zu unterhöhlen. Diese Gefahr hat auch die Bundesregierung in der Antwort auf eine Kleine Anfrage der FDP im Oktober 2019 skizziert. Deep Fakes können demnach „eine große Gefahr für Gesellschaft und Politik darstellen“, wenn sie genutzt werden, um die öffentliche Meinung und den politischen Prozess zu beeinflussen. Als Gegenmittel empfiehlt die Regierung, in erster Linie die Medienkompetenz zu verbessern. Fähigkeiten zur Identifizierung von Deep Fakes, die Zusammenarbeit von staatlichen Stellen, Privatwirtschaft, Zivilgesellschaft und Medien sowie die Resilienz gegenüber Desinformation müssten gestärkt werden.

Auf eine weitere Manipulationsmöglichkeit jenseits von Bild und Ton macht die Washingtoner Denkfabrik Carnegie Endowment for International Peace aufmerksam: via KI erstellte Texte. So ließen sich mit Leichtigkeit authentisch wirkende Social-Media-Konten erstellen, warnt der Thinktank. „Mit KI-generierten Profilfotos und KI-verfassten Beiträgen könnten die gefälschten Konten als menschlich durchgehen und echte Follower gewinnen. Ein großes Netzwerk solcher Konten könnte genutzt werden, um ein Unternehmen zu verunglimpfen und seinen Aktienkurs aufgrund der falschen Wahrnehmung einer Gegenreaktion der Basis zu senken.“

Finanzinstitute vorn dabei

Hoffnungen auf eine Wunderwaffe seien töricht, glaubt Carnegie. Technologische Lösungen könnten zwar helfen, aber auch die Gegenseite werde immer besser. Angesichts dieses Wettrüstens plädiert die Denkfabrik dafür, Mitarbeiter von Unternehmen zu schulen und mehr Kontrollen einzuziehen. Die Finanzindustrie sei schon etwas weiter als andere Branchen und profitiere von solidem Informationsaustausch und Krisenplanungen für Cybervorfälle, die auf Deep Fakes ausgeweitet werden könnten. Auch sei ein internationales Vorgehen vonnöten, um das Finanzsystem gegen Cyberbedrohungen jeder Art weiter zu stärken, so der Thinktank, der gemeinsam mit dem World Economic Forum eine internationale Strategie für Cybersicherheit zum Schutz des Weltfinanzsystems erarbeitet hat.