NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

KI und Biometrie verhindern Sozialhilfebetrug schon im Ansatz

Nuance Communications

3 Juni 2021

Betrüger:innen haben in ganz Europa die Unsicherheiten rund um COVID-19 ausgenutzt, um Milliarden an Hilfs- und Konjunkturgeldern abzugreifen. Deshalb fragen sich Regierungen und Banken: wie können wir unsere Bürger:innen und Kund:innen besser schützen? Immer mehr setzen dafür auf intelligente Lösungen auf Basis von KI und Biometrie, um Sozialleistungsbetrug proaktiv zu erkennen und zu verhindern und gleichzeitig sicherzustellen, dass berechtigte Antragsteller:innen ihre Leistungen erhalten.

Betrug war bereits vor der Pandemie ein ernstzunehmendes Problem: In einer im Januar 2020 veröffentlichten EU-weiten "Scams and Fraud"-Studie der Europäischen Kommission gab die Mehrheit (56 %) der Europäer:innen an, in den vergangenen zwei Jahren Betrügereien zum Opfer gefallen zu sein.

Und dann kam COVID-19. Die weitreichenden negativen Auswirkungen der Pandemie auf die Wirtschaft eröffneten Betrüger:innen viele neue Möglichkeiten – vor allem im Zusammenhang mit Leistungsbetrug bei Arbeitslosengeldern.

Unbürokratische Verteilung von Hilfsmitteln lockt

Kriminelle an

Die Krise ließ den EU-Arbeitsmarkt dramatisch schrumpfen: Im zweiten Quartal des letzten Jahres gingen in der gesamten EU 5,5 Millionen Arbeitsplätze verloren. Da sich die Regierungen beeilten, neue Hilfs- und Konjunkturprogramme – von Spaniens ETRE bis Großbritanniens "Furlough"-Programm – umzusetzen, wurden Antragsprozesse vielerorts vereinfacht, um den Verwaltungsaufwand zu reduzieren und hilfsbedürftige Bürger:innen zeitnah zu unterstützen.

Professionelle Betrüger:innen nutzten diese Situation jedoch schnell zu ihrem Vorteil aus und reichten Anträge auf Arbeitslosenunterstützung und Unternehmenszuschüsse im Namen fremder Personen und Firmen ein. So stahlen Kriminelle in Frankreich 1,7 Millionen Euro, die zur Unterstützung von gefährdeten Unternehmen gedacht waren. In Deutschland erbeuteten Betrüger:innen mindestens 31,5 Millionen Euro von einer einzigen Landesregierung. Und in Großbritannien wurden schätzungsweise bis zu 3,5 Milliarden Pfund an COVID-Hilsmitteln in betrügerischer Absicht beantragt oder fälschlicherweise ausgezahlt.

Das sind nur einige Beispiele, die zeigen, wie die COVID-19-Pandemie die Notwendigkeit eines Umdenkens in Bezug auf Authentifizierung und Betrugsprävention beschleunigt hat. Regierungsbehörden in ganz Europa – einschließlich in Großbritannien – nehmen dies zur Kenntnis, stellen größere Budgets für entsprechende Maßnahmen bereit und überlegen, was sie noch unternehmen können, um sich und ihre Bürger:innen zu schützen.

Verifizierung biometrischer Merkmale ist schneller und zuverlässiger

Eine mögliche Lösung ist KI-basierte Biometrie, die Bürger:innen authentifizieren kann und Betrüger:innen bei telefonischen und digitalen Interaktionen schnell und sicher erkennt. Im Vergleich zu Sicherheitsfragen oder der Überprüfung am Telefon sind biometrische Verfahren schneller und zuverlässiger bei der Authentifizierung und dem Entlarven von Betrüger:innen, da sie sich nicht durch gestohlene Angaben täuschen lassen. Stattdessen verifizieren sie Personen auf Grundlage von individuellen Merkmalen. Noch effektiver ist die Verknüpfung von Biometrie mit anderen Funktionen wie Umgebungserkennung (Überprüfung des Geräts, des Netzwerks, des Kanals und des Standorts) und Anti-Spoofing-Maßnahmen (Verhinderung von ANI-Spoofing und Erkennung synthetischer Sprach- oder Audiowiedergaben).

Ein Beispiel: Eine Betrügerin oder ein Betrüger ruft dutzende Male in einem Contact Center an und gibt sich jedes Mal als eine andere Person aus, um Leistungsansprüche unter falschem Namen anzumelden. Wenn die Betrügerin oder der Betrüger über Identitätsdaten anderer Personen verfügt (die oft leicht im Dark Web erhältlich sind), kann sie oder er unentdeckt bleiben und sich Tausende Euro an staatlicher Unterstützungen erschleichen.

Wird das Contact Center jedoch durch eine Biometrielösung unterstützt, erkennt diese Betrüger:innen innerhalb von Sekunden und alarmiert die jeweiligen Contact Center-Mitarbeiter:innen in Echtzeit. In der Zwischenzeit kann das Sicherheitsteam historische Anrufaufzeichnungen analysieren und feststellen, ob dieselbe Stimme schon häufiger in Anrufen aufgetaucht ist. Das Team kann dann die Stimme einer Überwachungsliste hinzuzufügen, sodass die Betrügerin oder der Betrüger beim nächsten Anruf sofort erkannt wird. Das ermöglicht auch das Sammeln hochwertiger Beweise für die Strafverfolgung.

Investitionen in die digitale Zukunft

Auch der Blick in die Zukunft über die Pandemie hinaus zeigt die Bedeutung von Lösungen gegen diese Art von Betrug. Regierungsbehörden müssen ihre Bürger:innen in diesem Übergang zur "neuen Normalität" im Jahr 2021 proaktiv schützen. Vorausschauende Investitionen in Technologien der nächsten Generation wie KI und Biometrie können dazu beitragen, Interaktionen mit Bürger:innen und Kund:innen zu optimieren und zu schützen, sodass sie Leistungen schneller erhalten und Betrüger:innen keine Chance haben.

Hier gibt es weitere Informationen zu Sicherheits- und Biometrielösungen von Nuance. Darüber hinaus stehe ich Ihnen auch gerne für ein Gespräch zur Verfügung, um die spezifischen Herausforderungen Ihrer Behörde zu besprechen und wie unsere Technologien bei Ihnen am besten eingesetzt werden können.

Tags: Biometrische Authentifizierung

More Information

KI und Biometrie bietet verbesserten Schutz gegen Sozialhilfebetrug

Sprechen Sie uns an

Learn more