PRESSEMITTEILUNG

KYC hoch drei für Sicherheit in unsicheren Zeiten

Wien, 10. April 2025 – In Zeiten intensiver digitaler Vernetzung und zunehmender Cyberbedrohungen, auch aufgrund krisenhafter globaler politischer Entwicklungen, stehen demokratische Gesellschaften vor großen Herausforderungen. Insbesondere die wechselseitige Abhängigkeit von regionalen, nationalen und globalen Wirtschaftsräumen verlangt nach hochsicheren Methoden wie etwa sichere Know-Your-Customer-(KYC-)Verfahren, um effiziente und sichere digitale Geschäftsprozesse zu gewährleisten.

Markus Vesely, CEO des Vertrauensdiensteanbieters A-Trust, sieht hiervon insbesondere drei Sektoren besonders stark betroffen: *„Banken und Finanzinstitute müssen die Identität und Aktivitäten ihrer Kunden überprüfen und Geldwäscherisiken bewerten. Der Immobiliensektor zieht auch aufgrund seiner immensen Größe – laut Statista[1)] wird er 2025 global einen Wert von etwa 596,26 Bio. Euro erreichen – naturgemäß Kriminelle an, die ihn zur Geldwäsche und Terrorismusfinanzierung nutzen. Und für E-Commerce und Online-Dienstleister ist KYC zwar nicht immer gesetzlich vorgeschrieben, aber es dient zur Betrugsprävention und stellt sicher, dass Personen, die Güter auf digitalen Plattformen kaufen oder Online-Services beanspruchen, auch wirklich die sind, für die sie sich ausgeben*."

Deepfake kann biometrische Verfahren überlisten

Im traditionellen KYC sorgt die persönliche Identifizierung und die Vorlage physischer Dokumente für einen hohen Sicherheitsgrad, der in der elektronischen Welt per Fernverifizierung mithilfe digitaler Tools wie optischer Zeichen-, Gesichts- und Liveness-Erkennung erreicht werden soll – und bisher auch wurde. Doch nun hat die rasante Entwicklung der Künstlichen Intelligenz diese Barriere porös gemacht und öffnet Betrüger:innen, die Deepfake-Technologie nutzen, neue Türen. Die gängigsten Methoden umfassen

- **Gesichtsaustausch und vollständig generierte Identitäten**: KI kann Gesichter nahtlos ersetzen oder generieren, um sie an gestohlene Ausweisdokumente anzupassen. Diese Fälschungen können Lichtbildausweisvergleiche und Gesichtserkennungssysteme umgehen.
- **Klonen von Stimmen**: Stimmen werden repliziert, um Stimmauthentifizierungsprotokolle zu umgehen, insbesondere im Finanzdienstleistungsbereich, wo Stimmverifizierung üblich ist.
- **Erstellung synthetischer Dokumente:** Im Darknet verkaufte Tools bieten die Möglichkeit, Identitätsdokumente realistisch zu fälschen, komplett mit Pseudo-Live-Videomaterial. So können Betrüger:innen Konten unter falschen Identitäten eröffnen.
- **Kompromittierung der Liveness-Erkennung**: Fortschrittliche Deepfake-Algorithmen imitieren menschliche Handlungen wie Blinzeln oder Lächeln, um Systeme zu täuschen, die die Anwesenheit eines lebenden Menschen bestätigen sollen.

Welche Maßnahmen können nun die Wahrscheinlichkeit eines erfolgreichen Einsatzes von Deepfakes verringern?

Gegenmittel: Authentifikation via ID Austria

„Der Schlüssel liegt in der Authentifizierung der Nutzer:innen mittels ID Austria", erklärt Markus Vesely: *„Die österreichische eID ermöglicht eine sichere und eindeutige Identifikation in Online-Verfahren. Unternehmen und Behörden können diese nach der Anbindung nutzen, um beispielsweise ihren KYC- bzw. ReKYC-Pflichten sicher, verlässlich und DSGVO-konform nachzukommen oder Nutzenden den Zugang zu den eigenen eServices zu ermöglichen."*

Insbesondere da für die Registrierung der ID Austria eine Registrierungsbehörde aufgesucht werden muss, um seine Identität feststellen zu lassen und die Anwendung mit seinem Smartphone zu

verknüpfen, bietet eine Identifikation im Rahmen des KYC-Verfahrens mit dieser eID keine Angriffsfläche für Deepfakes. *„Die ID Austria ist eindeutig einer Person zugeordnet und von vertrauenswürdiger Quelle bestätigt.“,* so der A-Trust-CEO.

Ein KYC-Verfahren per Multifaktorauthentifizierung durchzuführen, sieht er als grundsätzlich sicherste Methode. Dafür sind jeweils drei Komponenten notwendig und bei der Nutzung der ID Austria drei Kombinationen möglich:

- Signaturpasswort und Geräte-PIN oder
- Signaturpasswort und Biometrie oder
- Signaturpasswort und FIDO-Token

1) https://de.statista.com/outlook/fmo/immobilien/weltweit

Über A-Trust
Compliance, Integrität, Komfort und vor allem Sicherheit: A-Trust ist ein zuverlässiges Partnerunternehmen, wenn es um Sicherheit im digitalen Raum geht, und steht für innovative und professionelle Zertifikats- und Signaturlösungen. Das Unternehmen ist ein qualifizierter Vertrauensdiensteanbieter für elektronische Zertifikate auf Basis der eIDAS-Verordnung und in der EU-Trusted List eingetragen.

Mit mehr als 25 Jahren Erfahrung im Zertifikatsbereich und mehr als 4 Millionen aktiven Nutzer:innen einer A-Trust-QES (z.B. ID Austria) steht A-Trust für Beständigkeit und Investitionssicherheit und ist auch im Heimatmarkt Österreich zum Branchenführer avanciert. Gemeinsam mit verschiedenen internationalen Partner:innen bietet A-Trust erfolgreich sichere und komfortable Signaturlösungen für zahlreiche Kund:innen in der DACH-Region und in ganz Europa an. www.a-trust.at

Rückfragehinweis

A-Trust GmbH
Mag. Eva Kleinbrod, MSc
Head of Marketing & PR
Landstraßer Hauptstraße 1b / E02
1030 Wien
Tel.: +43 1 713 21 51 341
E-Mail: eva.kleinbrod@a-trust.at

corporate identity prihoda gmbh
mag. irmgard dober
pr consultant
peter-jordan-straße 74
1190 wien
tel.: +43 1 479 63 66–22
e-mail: irmgard.dober@cip.at