RIO

Resilienz im Onlinehandel

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2021	**Status**	abgeschlossen
Projektstart	01.11.2022	**Projektende**	31.12.2024
Zeitraum	2022 - 2024	**Projektlaufzeit**	26 Monate
Keywords	Cybercrimeprevention, KI-basierte-Detektionsverfahren, Mobile-Resilienz, Natural-Language-Processing, Cryptowährungsinvestbetrug		

Projektbeschreibung

Die Umsätze im Onlinehandel sind mit 9,6 Milliarden in Österreich (+20%) und 99,1 Milliarden Euro DE (+19%) auf einem Allzeithoch. Der Anteil, der über mobile Endgeräte erwirtschaftet wird, stieg dabei signifikant um 67 Prozent auf 2 Milliarden in Österreich, in Deutschland macht dieser bereits 40,2 Prozent des erwirtschafteten Umsatzes aus. Mehr als jeder zweite Euro wird dabei über große Online-Marktplätze umgesetzt. [BEVH 2022][HAV 2021] Dem gegenüber steht die rapide Zunahme an Cybercrime-Delikten (2020: +26,3%). Für Konsument:innen sind derzeit zwei Themen von neuralgischer Bedeutung: Der Bestellbetrug, durch Fake-Shops sowie der Betrug durch Investment-Plattformen, der einhergehend mit der Beliebtheit von Kryptowährungen zunimmt. [BMI 2021]

Fake-Shops verursachen großen, volkswirtschaftlichen Schaden, eine Dunkelfeldstudie geht von 320.000 direkt betroffenen Konsument:innen in Österreich aus und beziffert die Schadenhöhe auf 16 Millionen Euro. [KFV 2021] Risikogruppen wie Personen mit höherem formalem Bildungsniveau und Risikoverhalten beim Surfen, machen den Großteil der Opfer von Fake Shops aus. Männer im Alter von 18 bis 29 Jahren bilden die sorgloseste Risikogruppe. Umso wichtiger ist, dass diese Gruppen vermehrt technische Sicherheitsmaßnahmen einsetzen und ihre Wachsamkeit erhöhen. [KFV 2021]

Das KIRAS-Projekt SINBAD, hat erfolgreich einen auf Künstlicher Intelligenz (KI) basierenden Fake-Shop-Detector entwickelt, für Konsument:innen steht dieser kostenlos als Browser-Plugin für Edge, Firefox und Chrome zum Download bereit. An der laufenden Beta-Phase beteiligen sich bereits über 6000 Konsument:innen und schützen damit nicht nur sich selbst, sondern auch andere und tragen somit bereits erfolgreich zur rascheren Exponierung von betrügerischen Onlinehändlern bei. Die hierbei im Einsatz befindlichen KI-Modelle erzielen im Praxiseinsatz auf über 400.000 Websites eine Genauigkeit der korrekten Klassifikation von 91%. [BLD+ 2020] Dem trainierten KI-System stehen dabei über 21.000 Merkmale für die Entscheidungsfindung zur Verfügung. Die Stärke des Verfahrens liegt darin, dass kein Einzelnes hierbei heraussticht, sondern, dass gerade die Kombination einer Vielzahl von Einzelmerkmalen, ihr Vor¬handensein oder Nicht-Vorhandensein, zu einer sehr robusten Risikobewer¬tung durch die KI führt.

Das Projekt „Resilienz im Online-Handel“ (RIO) setzt die erfolgreiche Präventionsarbeit durch zielgerichtete Innovationen entlang des Fake-Shop Detection-Lifecycles fort. Diese umfassen:

(1) Eine modular, skalierbare und einfach zu erweiterbare Open Source-Plattform für KI-basierte Risk-Assessment Services

und deren Anwendungen im qualitätsgesicherten Praxiseinsatz.
(2) Einen Community-enabled Fraud-Prevention Ansatz: Durch den Einsatz der KI-Detektion erreichte die Anzahl der veröffentlichten Warnmeldungen einen neuen Höchststand. Hierbei gilt es Expert:innen zu entlasten, indem Aufgaben der Qualitätssicherung durch geeignete Gamification und Nudging Ansätze in Form einer Spielumsetzung an die Community delegiert werden.
(3) Die Realisierung einer minimal-invasiven App-basierten Lösung zum Echtzeitschutz vor Betrugsfallen zur Steigerung der Mobilen-Resilienz erfolgt unter Berücksichtigung hoher Privatsphäre-Standards.
(4) Die Erarbeitung von Demonstratoren mit Schwerpunktsetzung auf Natural Language Processing (NLP) zur Steigerung der menschlichen Nachvollziehbarkeit KI basierter Risiko-Bewertungen, der Auffindung zusammenhängender Betrugsfälle (Cluster) sowie der Betrugsprävention auf Online-Marktplätzen. Dies erfolgt unter Begleitung der Bedarfsträger BMSGPK und BMI und umfasst auch die Evaluierung des Einsatzpotenzials dieser Tools für Stakeholder hinsichtlich ihrer ergänzenden Wirkung der Präventionsarbeit und Kriminalitätsbekämpfung.
(5) Die Analyse betrügerischer Kryptowährung-Investment-Plattformen zum Schutz vor dieser wachsenden Bedrohung für Konsument:innen, durch die bereits erfolgreich eingesetzten Methoden der Fake-Shop Detektion.
(6) Die Schaffung einer Wissensgrundlage über zwei Studien zu „soziodemografischem Faktoren KI basierter Vertrauenskalibrierung“ sowie zu „Dunkelfeldstudie Betroffener, Betrugsmuster und Grauzonen im Online-Handel“, die weiterführende evidenzbasierte Präventionsmaßnahmen zu Betrugsdelikten im Online-Handel ermöglichen.

Abstract

Online sales are at an all-time high at EUR 9.6 billion in Austria (+20%) and EUR 99.1 billion in Germany (+19%). The share that is generated via mobile devices rose significantly by 67 percent to 2 billion in Austria, in Germany this already accounts for 40.2 percent of generated sales. More than every second euro is spent on large online marketplaces. [BEVH 2022][HAV 2021] On the other hand there has been further increase in cybercrime offenses (2020: +26.3%). Two issues are hereby of neuralgic importance for consumers: fraud by fake shops and fraud by fake investment platforms, which is increasing in line with the popularity of cryptocurrencies. [BMI 2021] Fake shops cause great economic harm; a dark field study assumes 320,000 directly affected consumers in Austria and estimates the amount of damage at 16 million euros. [KFV 2021] Risk groups such as people with a higher level of formal education and risky behavior when surfing, make up the majority of victims of fake shops. Men between the ages of 18 and 29 form the most carefree risk group. It is all the more important that these groups protect themselves through technical security measures and increase their vigilance. [KFV 2021]
The KIRAS project SINBAD has successfully developed a fake shop detector based on artificial intelligence (AI). This is available for consumers to download free of charge as a browser plugin for Edge, Firefox and Chrome. More than 6000 consumers are already participating in the current beta phase, hereby protecting not only themselves but also others and thus already successfully contributing to the faster exposure of fraudulent online retailers. The AI models in place achieve an accuracy of 91% in practical use proven on over 400,000 websites. [BLD+ 2020] The trained AI system has over 21,000 features available for decision-making. The strength of the method lies in the fact that no individual feature stands out, but that the combination of a large number of individual characteristics, including their presence or non-existence, leads to a very robust risk assessment by the AI.

The project "Resilience in Online Trade" (RIO) continues the successful preventive work through targeted innovations along the fake shop detection lifecycle. These include:
(1) A modular, scalable and easily expandable open-source platform for AI-based risk assessment services and their

applications for quality-assured practical use.
(2) A community-enabled fraud prevention approach: Through the use of AI detection, the number of published warnings reached a new high. It is important to support and relieve experts by delegating quality assurance tasks to the community, achieved via suitable gamification and nudging approaches in the form of an online game.
(3) The implementation of a minimally invasive app-based solution for real-time protection against fraudulent e-commerce increases the mobile resilience while maintaining high privacy standards.
(4) The development of demonstrators with a focus on Natural Language Processing (NLP) aim to increase the human explainability of AI-based risk assessments, detect related fraudulent instances (clusters) and implement fraud prevention measure on large online marketplaces. This is done with the support of the BMSGPK and BMI and includes the evaluation of the demonstrated potential in the stakeholder’s context with regard to supplementary effects of existing preventative and investigative measures.
(5) Porting and applying successfully used tools and methods from the fake shop detection scenario to the domain of fraudulent cryptocurrency investment platforms to build up protective measures against this growing threat to consumers.
(6) Building up knowledge for targeted preventative measures, via two studies on "sociodemographic factors of AI-based trust-calibration" and a "dark field study of those affected, exposing fraud patterns and gray areas in online trade”

Endberichtkurzfassung

Der Fake-Shop Detector konnte im Rahmen des RIO-Projekts wesentlich weiterentwickelt und als zentrale Präventionsplattform gegen Fake-Shops etabliert werden. Mit über 10.000 täglichen Nutzer:innen, Risikobewertungen zu über 1.8 Millionen analysierter Domains und einer aktiven Schutzfunktion vor betrügerischen Onlineshops hat sich das System als wirkungsvolles Instrument zum Schutz von Konsument:innen erwiesen. Im Mittelpunkt des Projekts stand die Entwicklung einer modularen, skalierbaren Plattform, welche erfolgreich umgesetzt wurde. Die Plattform integriert heterogene Datenquellen, verarbeitet diese über eine robuste Datenpipeline und stellt die Ergebnisse für unterschiedliche Frontends bereit.

Ein zentraler Erfolgsfaktor war die umfassende Überarbeitung und Erweiterung des Shop-Check-Tools, das erklärbare Risikofaktoren wie Impressumsinformationen, Nutzerbewertungen und rechtliche Auffälligkeiten aggregiert und für Endnutzer:innen transparent darstellt. Ergänzt wurde dies durch halbautomatische Crawler, die Scam-Quellen kontinuierlich überwachen und so die Datenqualität und Aktualität sichern. Diese Community-gestützte Betrugsprävention wurde durch Partnerschaften und durch die Integration privater Warnlisten erheblich gestärkt.

Im Bereich der mobilen Resilienz wurde eine App-Prototyp für Android entwickelt und in einer Nutzer:innenstudie umfassend getestet. Parallel dazu wurde das Browser-Plugin verbessert und unter anderem mit Push-Benachrichtigungen und Mehrsprachigkeit ausgestattet. So konnten insbesondere mobile Nutzer:innen besser vor Betrug geschützt werden.

Wissenschaftlich wurde das Projekt durch umfassende Experimente im Bereich Fake-Shop-Clustering ergänzt. Mehrere KI-Methoden (K-Means, Agglomerative Clustering, HDBSCAN) wurden auf einen Datensatz von 23.800 archivierten Shops angewendet. In Zusammenarbeit mit Watchlist Internet konnte eine Ground-Truth erstellt und für die Evaluation genutzt werden. Auch ein Proof-of-Concept zur Erkennung von Kryptowährungs-Investmentbetrugsseiten wurde durchgeführt.

Zwei begleitende Studien – eine Evaluierungsstudie mit 497 Teilnehmer:innen und eine Dunkelfeldstudie zu Grauzonen im

Onlinehandel – belegten den Nutzen und die gesellschaftliche Relevanz der entwickelten Werkzeuge. Der finanzielle Schaden durch Fake-Shops in Österreich wurde auf mindestens 7,85 Mio.?€ pro Jahr geschätzt.

Abgerundet wurde das Projekt durch zahlreiche Disseminationsmaßnahmen, internationale Vernetzung sowie die Auszeichnung mit dem Staatspreis Digitalisierung , dem Constantinus Award und dem eAward . Der Fake-Shop Detector wurde von AV Comparatives zudem als wirksamstes Tool gegen Internet-Fake-Shops bewertet – ein starkes Zeichen für die Bedeutung der RIO-Ergebnisse im digitalen Verbraucherschutz.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- cyan Security Group GmbH
- Österreichisches Institut für angewandte Telekommunikation
- Xylem - Science and Technology Management GmbH
- X-Net Services GmbH
- Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
- Bundesministerium für Inneres