DAMOVO

Use Case

PENETRATION TESTING FÜR KI-GESTÜTZTE VOICEBOTS BEI EINEM REISEUNTERNEHMEN

HERAUSFORDERUNGEN

Ein großes, international tätiges Reiseunternehmen mit rund 50.000 Mitarbeitenden setzte zunehmend auf KI-gestützte Voice- und Chatbots, um den Kundenservice bei Buchungen, Umbuchungen, Rückerstattungen und Reiseunterbrechungen zu automatisieren. Die eingesetzten Voicebots eröffneten jedoch eine weitgehend ungeprüfte Angriffsfläche.

Klassische Penetration-Testing-Tools konnten telefonbasierte Interaktionen nicht ausreichend prüfen. Manuelle Red-Team-Tests wiederum ließen sich nicht effizient skalieren.

Neue Risiken wie Prompt-Injection-Angriffe über Sprache, Fehlinterpretationen durch automatische Spracherkennung, Social Engineering und Datenabfluss wurden durch bestehende Sicherheitskonzepte nicht systematisch abgedeckt.

UMSETZUNG

Der Kunde nutzte eine agentenbasierte Plattform für Voicebot-Penetration-Testing als Managed Service.

Die Lösung generierte automatisch Hunderte Angriffsszenarien auf Basis der OWASP GenAI Top 10. Anschließend führte sie reale Testanrufe gegen den produktiven Voicebot durch, zeichnete beide Audiokanäle auf, transkribierte die Gespräche und bewertete die Ergebnisse mithilfe von KI als unabhängige Sicherheitsinstanz.

Jede Interaktion wurde analysiert, nach Risikostufe und Angriffsvektor kategorisiert und mit vollständigen Nachweisen in strukturierten Sicherheitsberichten dokumentiert.

VORTEILE

Das Reiseunternehmen erhielt eine kontinuierliche und skalierbare Sicherheitsprüfung für seine KI-gestützten Voicebots. Dabei wurden Hunderte Angriffsvektoren abgedeckt, deren manuelle Prüfung sonst Monate gedauert hätte.

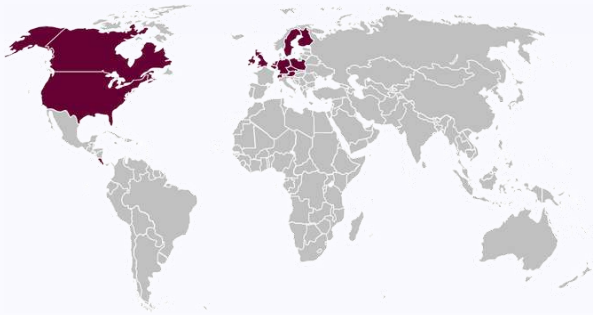
Sicherheitslücken, die speziell bei sprachbasierter KI auftreten, konnten frühzeitig erkannt werden.

Gleichzeitig stärkte das Unternehmen seine Ausrichtung an neuen GenAI-Sicherheitsstandards und reduzierte operative Risiken sowie Reputationsrisiken deutlich.

Der Managed Service sorgt für ein hohes Sicherheitsniveau im Unternehmenseinsatz von KI, ohne den laufenden Kundenservice zu unterbrechen.

ÜBER DAMOVO

Damovo ist ein globaler Technologie-Dienstleister, der Unternehmen weltweit bei ihrer digitalen Transformation unterstützt. Das breite Portfolio umfasst Lösungen in den Bereichen Cybersicherheit, Unternehmensnetzwerke, Unified Communications und Collaboration, Contact Center und globale Managed Services.



Mit über 600 engagierten Mitarbeitenden ist Damovo in Europa, Amerika und der Asien-Pazifik-Region tätig und bietet globalen Support in mehr als 150 Ländern.

LET'S CONNECT

Mehr Informationen über Damovo finden Sie auf unserer Webseite.

www.damovo.com

Oder nehmen Sie Kontakt mit uns auf.

connect@damovo.com