Foto: © fotokitas / Adobe Stock

Starke Authentifizierung für Call Center

Schwachstellen schließen

Gut Ding will Weile haben – so sagt der Volksmund. Das trifft auch in Sachen Authentifizierung bei telefonischen Transaktionen zu, doch die Medaille hat zwei Seiten. Kunden möchten nicht unnötig warten, wenn sie sich in der Hotline eines Anbieters oder Dienstleisters zu erkennen geben (müssen). Schneller und vor allem sicherer geht das heute mit einer so genannten Multi-Faktor-Authentifizierung im Call Center. Wie die Kombination verschiedener Identifizierungsmöglichkeiten funktioniert, erfahren Sie hier.

Schneller, direkter und effizienter Kundenservice ist das wichtigste Ziel von Call Center-Betreibern. In der Wahrnehmung vieler Konsumenten ist die Abwicklung von Transaktionen über ein Call Center aber teilweise immer noch mit Frustrationen und einem vergleichsweise hohen Zeitaufwand verbunden. Für Unternehmen und Finanzinstitute ist dies ein Problem, denn „Zeit" ist für Kunden oftmals ein Gradmesser für die Qualität: In einer Studie des Marktforschungsinstituts Forrester Research gaben 73 Prozent der befragten Konsumenten an, dass die Wertschätzung ihrer Zeit der ausschlaggebende Faktor für die positive Bewertung von Interaktionen ist.

Eine zentrale Rolle spielt dabei die Authentifizierung eingehender Anrufe. Einerseits trägt der hierfür benötigte Zeitaufwand dazu bei, dass Kunden die Interaktion als umständlich empfinden. Dies gilt insbesondere, wenn ältere Systeme in den Prozess involviert sind. Andererseits hat die zuverlässige Authentifizierung von Anrufern für Banken, Unternehmen und letztendlich auch für den Kunden höchste Priorität. Die sehr hohen Beutesummen, die durch Cyberkriminalität mittlerweile erzielt werden können, haben eine neue Art deutlich raffinierterer Angreifer angelockt. Systematisch werden heute die Schwachstellen von Organisationen identifiziert und dann gezielt angegriffen. Als verwundbarste Komponente erweist sich dabei oftmals der Telefonkanal – also das Call Center.

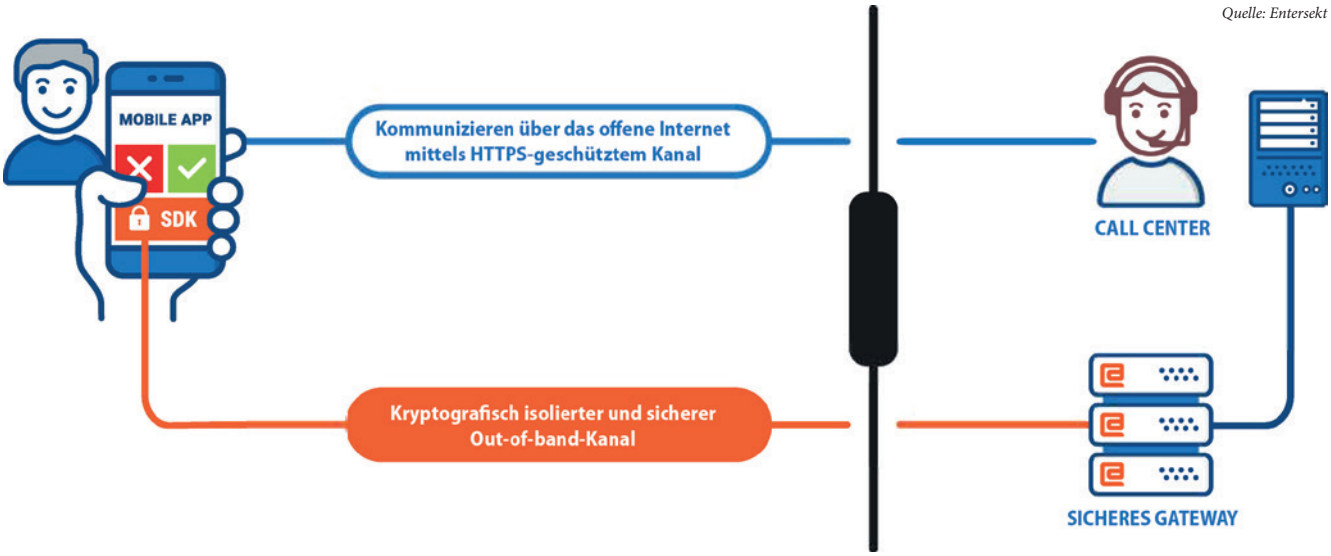
Angriffe über den Telefonkanal sind meist Teil einer so genannten Omni-Kanal-Strategie, mit der Betrüger auf sensible Daten abzielen. So können Angreifer zum Beispiel zunächst Social Engineering einsetzen, um das Passwort für das Konto eines Opfers zurückzusetzen. Mit diesem Passwort sind dann im Anschluss verschiedene Formen von Online-Betrug möglich. Der Wechsel zwischen verschiedenen Kanälen macht es dabei erheblich schwerer, Betrugsversuche zu identifizieren. Isoliert betrachtet, scheinen die einzelnen Transaktionen seriös zu sein, erst durch einen Blick auf alle Schritte wird der Angriff erkennbar.

Call Center in der Zwickmühle

Bislang standen Call Center vor der Herausforderung, genau die richtige Balance zwischen Sicherheit und Kundenservice zu finden. Herkömmliche Maßnah-

MEHRERE FAKTOREN KOMBINIEREN

Quelle: Entersekt



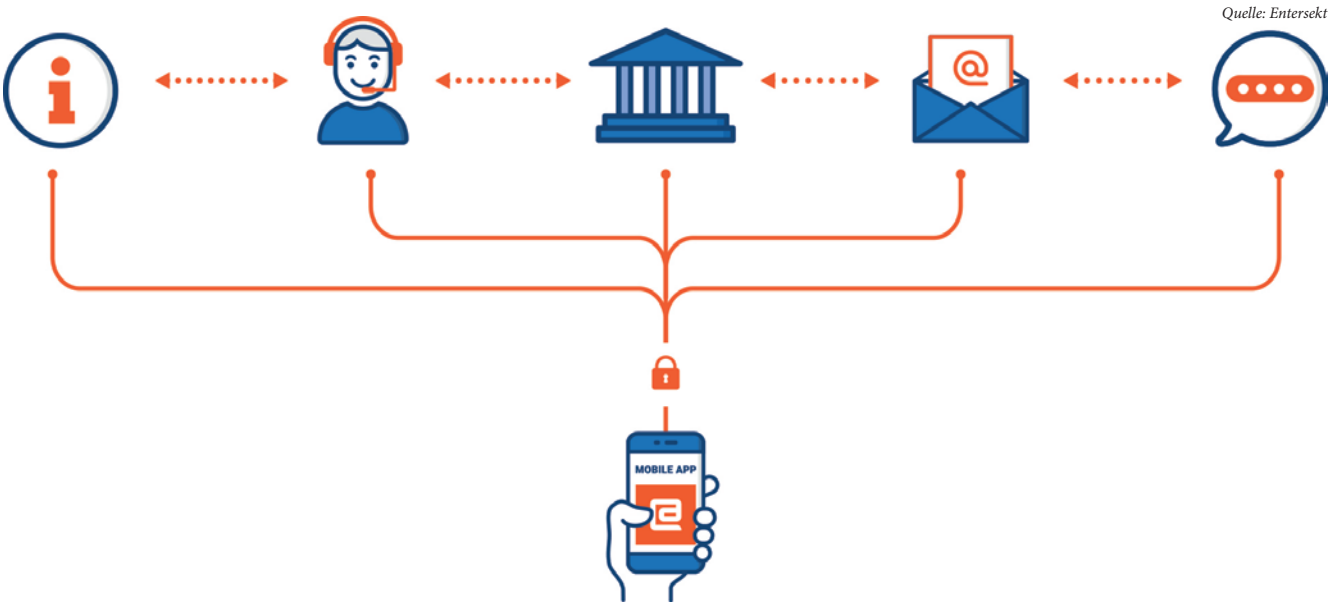
So sieht eine sichere Authentifizierung über das Mobiltelefon aus: Über den zusätzlichen Authentifizierungsfaktor – nämlich das spezifische Endgerät des Nutzers – wird die Erkennung eines Anrufers noch genauer.

men für eine starke Sicherheit durch mehrere Authentifizierungsfragen wirken sich fast unvermeidlich negativ auf die Kundenerfahrung aus, was Banken und Unternehmen natürlich vermeiden möchten. Dadurch wächst die Versuchung, Datenschutz und Sicherheit weniger konsequent umzusetzen – wodurch nicht nur das Risiko eines Angriffs steigt, sondern auch rechtliche Konsequenzen drohen.

Konsumenten verlangen nach schnellen, reibungslosen Prozessen. Bequemlichkeit wird im Vergleich zu Sicherheit priorisiert, wie sich zum Beispiel an häufig verwendeten Passwörtern ablesen lässt. Trotz aller Warnungen nutzen Anwender immer noch hartnäckig schwache Passwörter oder dasselbe Passwort für mehrere Online-Angebote. Diese Präferenz führt dazu, dass Anbieter im Wettbewerb ebenfalls Bequemlichkeit priorisieren. Gleichzeitig werden die bestehenden Sicherheitsanstrengungen der Anbieter durch schwache Passwörter unterminiert.

VIELSEITIGE EINSATZMÖGLICHKEITEN

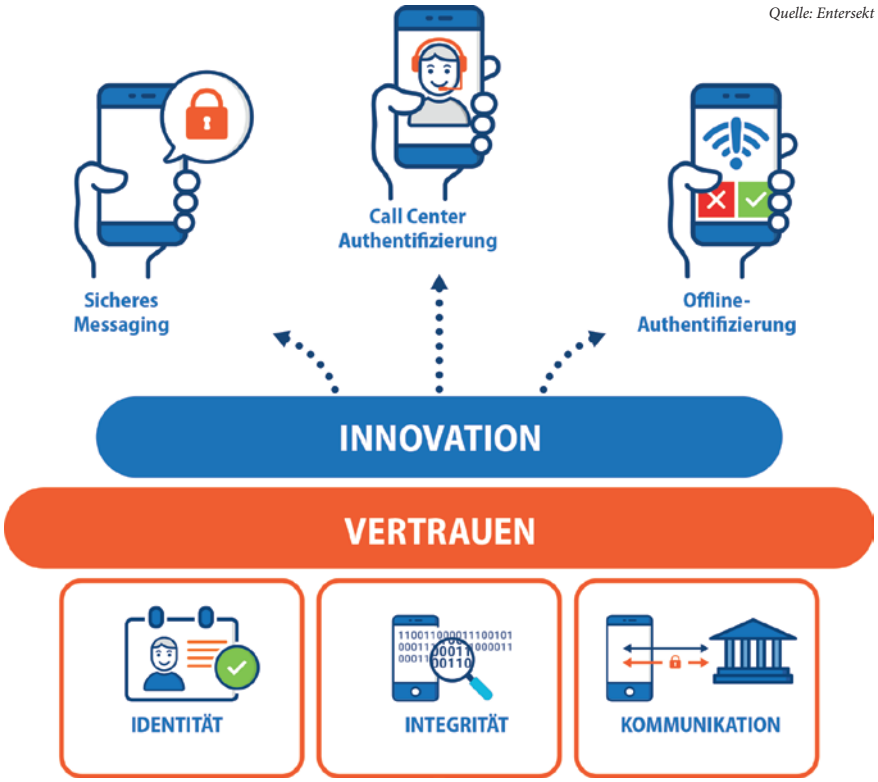
Quelle: Entersekt



Mit dem mobilen Endgerät können verschiedene digitale Prozesse authentifiziert werden.

INNOVATION BRAUCHT VERTRAUEN

Quelle: Entersekt



Eine sichere kanalübergreifende Kommunikation schafft Vertrauen und ist Voraussetzung für Innovation.

Wissensbasierte Authentifikation reicht nicht aus

Durch moderne Authentifizierungsmaßnahmen im Call Center wird es für Betrüger schwerer, Passwörter zurückzusetzen und unrechtmäßig erhaltene Log-in-Informationen für Web- und Mobile-Apps zu nutzen. Bei der telefonischen Anforderung neuer Passwörter setzen Call Center oftmals noch auf wissensbasierte Authentifizierungsmethoden (Knowledge-based Authentification, oder kurz KBA) in Form von vorher hinterlegten Frage-Antwort-Kombinationen: Wie lautet der Mädchenname der Mutter? Wie hieß das erste Haustier? In welcher Stadt wurde der Anwender geboren? Solche Informationen können von Angreifern zu leicht recherchiert werden, vielfach reichen bereits ein gründlicher Blick auf die Social Media-Profile der Anwender und ein wenig Social Engineering.

Um die bequeme, aber unsichere KBA abzulösen, haben einige Organisationen bereits Authentifizierungsverfahren implementiert, die auf biometrischer Stimmerkennung oder Einmal-Passwörtern basieren. In der Vergangenheit haben Cyberkriminelle aber leider schon bewiesen, dass sie mit neuen technischen Entwicklungen Schritt halten können. Sowohl Ein-Faktor-Authentifizierungsverfahren als auch Ein-Faktor-Stimm-Biometrie wurden bereits erfolgreich ausgetrickst. Für einen motivierten Betrüger ist es keine unüberwindbare Herausforderung, Stimmaufzeichnungen potenzieller Opfer im Internet aufzuspüren oder Software für die Stimmsynthese einzusetzen.

Authentifizierung per Mobiltelefon

Trotz Self Service- und Webchat-Angeboten werden Call Center auch zukünftig eine wichtige Aufgabe im Kundenservice erfüllen. Bestimmte Kundengruppen – häufig durch geringe Technik-Affinität gekennzeichnet – bevorzugen grundsätzlich die telefonische Interaktion. Gleichzeitig wächst ganz generell der Wert der menschlichen Interaktion beim Kundenservice, denn immer mehr direkte Berührungspunkte mit dem Anbieter verschwinden. Wie können Call Center also individuelle und gleichzeitig sichere Dienste anbieten?

Eine Möglichkeit besteht in der Verwendung eines zusätzlichen Authentifizierungsfaktors: dem Mobiltelefon. Die meisten Menschen in den Industrienationen haben heute im Alltag ihr Mobiltelefon jederzeit griffbereit. Über eine Lösung für starke Anwenderauthentifizierung mit digitalen Zertifikaten lassen sich registrierte Mobilgeräte eindeutig identifizieren, wobei die Authentifizierung über einen isolierten, geschützten Kanal (Out-of-band) stattfindet. Auf diesem Weg lassen sich Authentifizierungsfaktoren der folgenden drei Kategorien miteinander verbinden:

- Besitz (Possession): Mobiltelefon oder ähnliches Gerät
- Wissen (Knowledge): Passwort, KBA-Antworten etc.
- Eigenschaft (Inherence): Stimme etc.

Durch die Kombination zweier oder mehrerer Faktoren wird eine Multi-Faktor-Authentifizierung im Call Center ermöglicht, bei der Anrufer über das korrekte Gerät verfügen und sich zusätzlich per biometrischer Stimmerkennung oder Beantwortung von Sicherheitsfragen identifizieren müssen. Für Betrüger ist dies eine wesentlich höhere Hürde. Dieses Verfahren bedeutet zudem für Kunden keinen Mehraufwand, denn die Authentifizierung des Mobilgerätes verläuft im Hintergrund. Gleichzeitig wird dadurch der gesamte Authentifizierungsprozess beschleunigt und die durchschnittliche Anrufdauer verkürzt, wovon sowohl Kunden als auch Call Center-Betreiber profitieren. So kann eine Balance zwischen zuverlässiger Anrufer-Identifikation und positiver Kundenerfahrung erzielt werden.

Simon Rodway ←

AUTOR

Simon Rodway
ist Pre-Sales Solution Consultant UK bei Entersekt.

Web: www.entersekt.com/de
Mail: sales@entersekt.com