06.08.2026 – 09:01 Uhr

Neuer TrendAI-Report: Cyberkriminelle setzen zunehmend auf Insider statt auf Hacking

Neuer TrendAI-Report: Cyberkriminelle setzen zunehmend auf Insider statt auf Hacking

Untergrundmarkt für „Insider-as-a-Service" wächst: Preislisten, Vermittler und feste Geschäftsbeziehungen machen Vertrauen zur handelbaren Ware

Wallisellen, 6. August 2026 – TrendAI™, der Enterprise-Cybersecurity-Geschäftsbereich von Trend Micro, veröffentlicht den Report *„The Market for Trust: How Cybercriminals Recruit Corporate Insiders"*. Die zweijährige Analyse von Untergrundforen und Telegram-Kanälen zeigt: Cyberkriminelle versuchen Unternehmen zunehmend nicht mehr nur zu hacken, sondern deren Mitarbeitende zu kaufen. Besonders gefragt sind Beschäftigte bei Banken, Telekommunikationsanbietern, Social-Media-Plattformen und Krankenhäusern.

Für den Report haben die TrendAI-Forscher Mayra Rosario Fuentes, Stephen Hilt und David Sancho untersucht, wie sich der Handel mit Insider-Zugängen im Untergrund organisiert. Ihr Befund: Aus Einzelfällen ist ein reifes, arbeitsteiliges Geschäft geworden – mit Festpreisen, Gewinnbeteiligungen, Vermittlungsprämien und langfristigen Partnerschaften, die eher an eine reguläre Branche erinnern als an klassische Cyberkriminalität.

„Der einfachste Weg in ein Unternehmen führt heute nicht mehr zwangsläufig über eine Sicherheitslücke – oft reicht ein Mitarbeiter. In der Cybercrime-Untergrundszene wird vertrauenswürdiger Zugang zunehmend wie eine Ware gehandelt: Kriminelle werben gezielt Insider an, die Sicherheitsmassnahmen allein durch ihre reguläre Arbeit umgehen können. Sich gegen Insider-Bedrohungen zu schützen, bedeutet heute auch zu erkennen, dass die eigenen Mitarbeitenden selbst zum Angriffsziel geworden sind," erklärt David Sancho, Senior Threat Researcher bei TrendAI.

Die wichtigsten Erkenntnisse im Überblick

- **Insider-Rekrutierung ist heute ein eigener Wirtschaftszweig.** Auf Untergrundforen und in Telegram-Kanälen agieren Broker, Treuhänder-Dienste und feste Geschäftspartner mittlerweile so offen wie in einer regulären Branche.
- **Nicht die meisten Nutzerrechte zählen, sondern die grösste Entscheidungsmacht.**Kriminelle suchen gezielt nach Mitarbeitenden, die Zahlungen freigeben, Konten wiederherstellen oder Betrugsprüfungen umgehen können – Handlungen, die ein Angreifer von aussen niemals glaubwürdig nachstellen könnte.
- **Insider-Dienstleistungen werden zur Massenware.** Ob entsperrte Social-Media-Accounts, manipulierte Sendungsverfolgung oder erschlichene Rabatte: Für all das gibt es inzwischen feste Preise, garantierte Bearbeitungszeiten und sogar Wiederverkäuferprogramme.
- **Die KI-Branche rückt ins Visier.** Je mehr wertvolle Modelldaten, Trainingsmaterial und privilegierte Zugänge KI-Unternehmen anhäufen, desto attraktiver werden ihre Mitarbeitenden für Kriminelle.

„Lange Zeit haben wir bei Insider-Bedrohungen vor allem an frustrierte Mitarbeitende oder menschliche Fehler gedacht. Was wir heute beobachten, ist etwas grundlegend anderes: Kriminelle rekrutieren gezielt vertrauenswürdige Beschäftigte über organisierte Untergrund-Marktplätze und machen Insider-Zugänge zu einer Dienstleistung, die sich kaufen und verkaufen lässt", sagt Mayra Rosario Fuentes, Senior Threat Researcher bei TrendAI.

Der Report untersucht dieses Phänomen branchenübergreifend – von Behörden, Gesundheitswesen, Social Media, Telekommunikation und Finanzwesen über Industrie und Energie, Logistik und Einzelhandel bis hin zu Bewertungsplattformen. Wie weit die Professionalisierung bereits fortgeschritten ist, zeigt sich besonders deutlich an drei Branchen: Telekommunikation, Social Media und Finanzwesen. Hier dokumentiert der Report die konkretesten Fallbeispiele mit belastbaren Zahlen – teils bis hin zu strafrechtlicher Verfolgung.

- **Telekommunikation: Der SIM-Swap als lukrativstes Geschäft**

Ein bestochener Mitarbeiter kann per SIM-Swap die SMS-basierte Zwei-Faktor-Authentifizierung aushebeln und Angreifern so den Weg zu Bank- und Kryptokonten öffnen. Im Untergrund kostet das bei Verizon, T-Mobile oder AT&T bis zu 20.000 US-Dollar plus 20 Prozent Gewinnbeteiligung. Dass Strafverfolgungsbehörden bereits

reagieren, zeigt ein Fall aus den USA: Im November 2025 klagte die Staatsanwaltschaft Manhattan einen SIM-Swapping-Ring an, der mit bestochenen AT&T- und T-Mobile-Mitarbeitenden rund 435.000 US-Dollar von vier Opfern erbeutet haben soll.

- **Social Media: Gesperrte Accounts, entsperrt gegen Bargeld**

Insider reaktivieren gesperrte Accounts bei Meta, TikTok oder X für 1.000 bis über 7.000 US-Dollar oder winken betrügerische Werbeanzeigen durch. Bei Meta führte der Missbrauch des internen Tools „Oops“ durch bestochene Mitarbeitende Ende 2022 bei mehr als zwei Dutzend Beschäftigten und Vertragspartnern zu Entlassungen oder anderen disziplinarischen Konsequenzen. Meta verklagte die mutmasslichen Vermittler daraufhin 2023 vor einem kanadischen Gericht.

- **Finanzwesen: Schlüssel zum Bankkonto**

Ein Verkäufer bot in einem Untergrundforum dreijährigen Insider-Zugang zur Buchhaltung eines Unternehmens mit 25 Millionen US-Dollar Jahresumsatz an, Startgebot: 25.000 US-Dollar. Für die Vermittlung eines einzigen bestechlichen Mitarbeiters bei Kryptobörsen wie Binance oder Robinhood zahlten Auftraggeber bis zu 5.000 US-Dollar Kopfgeld oder alternativ 15 Prozent Beteiligung am Erlös.

Den vollständigen Report „*The Market for Trust: How Cybercriminals Recruit Corporate Insiders*” finden Sie hier: https://www.trendaisecurity.com/en/resources-insights/deep-research/what-cybercriminals-look-for-in-corporate-insiders

Pressestelle TrendAI™
c/o BRAND AFFAIRS AG

Mischa Keller / MSc Business Administration
Partner

Telefon: +41 44 254 80 00
E-Mail: trendmicro-media@brandaffairs.ch
Mühlebachstrasse 8 / 8008 Zürich / Switzerland

Weiteres Material zum Download

Bild: the_market_for_trust_fig06.jpg

Bild: the_market_for_trust_fig10.jpg