

## 4

## Persönliche Identitäten: Das geheime Schlupfloch in die Unternehmenssysteme



### Private Geräte werden zur Bedrohung für Organisationen ...

Persönliche Identitäten sind heute angreifbarer denn je. Schon immer waren Einzelpersonen die Zielscheibe von Cyberkriminellen, doch jetzt mit anderen Zielen und neuen Methoden. Heute nutzen sie persönliche Identitäten als Hintertüren, um in Unternehmensnetzwerke einzudringen. Beunruhigende **91 Prozent der Sicherheitsverantwortlichen in der DACH-Region gaben an, dass ihre Organisation bereits über persönliche Geräte oder Konten Ihrer Mitarbeitenden angegriffen wurde**. Solche Angriffe umgehen traditionelle Abwehrmechanismen, erweitern die Angriffsfläche und stellen ein nie dagewesenes Risiko für Organisationen dar.

Zusätzlich steht noch mehr auf dem Spiel, da die Cyberkriminellen ihre Angriffsmethoden skalieren. Durch den Einsatz von KI können sie ihre Angriffe auf Endverbraucher automatisieren, was es ihnen ermöglicht, mehrere kleinflächige, aber extrem gezielte Angriffe gleichzeitig auszuführen. Unsere globale Kundenumfrage zeigt, dass **73 Prozent der Befragten einen Anstieg bei den Angriffen auf Verbraucher festgestellt haben**. Mit ihren Angriffen auf Privatpersonen erbeuten die Cyberkriminellen zwar kleinere Beträge. Da diese Angriffe aber großflächig aufgesetzt sind, erreichen sie so letztlich ihre finanziellen Ziele.

### ... und selbst das persönliche Umfeld bleibt nicht verschont

Die Problematik wird immer dringlicher, da die Grenzen zwischen der privaten und beruflichen Nutzung von Geräten verschwimmen. Durch neue Arbeitsmodelle, wie Hybrid- und

Remote-Work, nutzen Mitarbeitende immer häufiger private Geräte und Konten für berufliche Zwecke – der Angriffsradius erstreckt sich weit über die Firewalls der Unternehmen hinaus.

Als wäre das nicht genug, haben Cyberkriminelle es durch großangelegte Datendiebstähle und den freizügigen Umgang mit persönlichen Daten im Netz leichter denn je, sensible Daten wie Passwörter, Adressen und Familienbande auszuspionieren. Über die Verwandten Ihrer Mitarbeitenden versuchen Angreifende heute, über Umwege in Ihre Organisation einzudringen. In einem aktuellen Fall zielten Cyberkriminelle mit SIM-Swapping auf das Kind einer Führungsperson ab, um so durch psychologische Manipulation Lösegeld zu fordern.<sup>1</sup> Nicht nur die Mitarbeitenden und Führungsetage werden zur Zielscheibe, sondern auch deren Familien.

Das Ergebnis: Auf die Einzelpersonen prasselt eine endlose Flut an großflächigen Betrugsmaschen ein, die die Wahrscheinlichkeit für menschliches Versagen in die Höhe treibt.



**Wir müssen über die Sicherheitsschulung im Unternehmen hinausgehen. Schulen Sie Ihre Familie und Ihre Freunde - denn Angreifer haben es auf jeden abgesehen.**



**Andrea Szeiler**  
Global CISO bei Transcom

<sup>1</sup> Golem (2024). Hacker erpressen Führungskräfte über Rufnummern ihrer Kinder.