Social Engineering: Fintechs im Fadenkreuz

München, 12.12.2019: Sind klassische Banken überholt? Fintechs, also Bezahldienste wie Paypal und Klarna oder Finanz-Startups wie N26, haben sich längst durchgesetzt und gehören für Millionen Deutsche zum Alltag. Durch ihre hohe Verbreitung finden allerdings auch Hacker diese Bezahldienste immer interessanter: Laut einer aktuellen Kaspersky-Studie nehmen sich Cyberkriminelle 2020 verstärkt Fintechs als Ziele vor.

Schon jetzt müssen Fintech-Anbieter strengste Compliance-Anforderungen erfüllen, da sie im Rahmen ihrer Dienstleistungen schützenswerte personenbezogene Daten sowie Finanzdaten speichern, übertragen und verarbeiten. Entsprechend empfindlich sind die Strafen bei Verstößen gegen diese Anforderungen: Erst im Mai 2019 hat die Berliner Datenschutzbehörde ein Bußgeld von 50.000 Euro gegen eine App-Bank verhängt[1].

Social Engineering: Schwachstelle Mensch

Müssen sich Fintechs im kommenden Jahr also noch stärker absichern als bisher? Die Experten von Kaspersky jedenfalls raten Anbietern dazu, ihr Augenmerk auf Cloud-Infrastrukturen zu legen und warnen explizit vor Social Engineering[2].

Was das bedeutet? Cloud-Security-Experte Dr. Hubert Jäger von der TÜV SÜD-Tochter uniscon GmbH klärt auf: „Beim Social Engineering manipulieren Cyberkriminelle ihre Opfer – meist mit der Absicht, an vertrauliche Informationen zu gelangen“. Auf diese Weise können die Angreifer zum Beispiel Zugangsdaten von Fintech-Mitarbeitern erbeuten. Mit diesen, so Jäger, könnten sich Hacker dann Zugriff zu den Systemen des Unternehmens verschaffen und dort etwa sensible Kundendaten entwenden oder manipulieren.

Besonders problematisch ist dies in Verbindung mit privilegierten Nutzerkonten, wie sie in vielen Rechenzentren und Unternehmen für Administrationsaufgaben vorgesehen sind. Denn diese Konten verfügen häufig über uneingeschränkte Zugriffsrechte. „Selbst, wenn die Daten verschlüsselt übertragen und gespeichert werden, müssen sie zur Verarbeitung unverschlüsselt auf den Unternehmensservern vorliegen. In diesem Zustand sind sie den Cyberkriminellen nahezu schutzlos ausgeliefert“, sagt Jäger.

Eigene Server sicherer als die Cloud?

Dabei spielt es keine Rolle, ob die Fintechs dazu auf externe Cloud-Infrastrukturen zurückgreifen oder Kundendaten im eigenen Rechenzentrum verarbeiten: Die meisten Server-Architekturen sehen privilegierte Admin-Zugriffe vor, die von Angreifern missbraucht werden können. Und vor den Methoden der Cyberkriminellen sind weder die eigenen Mitarbeiter noch die Mitarbeiter der Cloud-Dienstleister gefeit. Jäger: „Solange die Schwachstelle Mensch existiert, werden Hacker versuchen, sie auszunutzen“

Weiterführende Informationen und Beiträge zu den Themen Datenschutz, Datensicherheit und IT-Security finden Sie im privacyblog der uniscon GmbH.

---

[1] https://www.heise.de/newsticker/meldung/DSGVO-Verstoss-App-Bank-N26-soll-50-000-Euro-Bussgeld-zahlen-4431356.html

[2] https://securelist.com/ksb-2019/

uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.com

Pressekontakt

uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20