Datenschutz

Risiken durch Tracking beim Online-Banking

Dass Webseiten Dienstleistungen von Drittanbietern nutzen, um detaillierte Daten und Statistiken über ihre Nutzer zu bekommen, ist inzwischen Usus. Beim Online-Banking hat der Datenschutz jedoch einen besonderen Stellenwert. Wie es dort um die Nutzung von Drittanbietern zum Tracking bestellt ist, hat die Clicqz GmbH, München, untersucht. Zwölf Banking-Portale wurden auf Javascript oder Tracking-Pixel, auf den Ladekontext und das verwendete Tracking hin untersucht.

Dabei wurde nicht beurteilt, wie vertrauenswürdig die dritten Parteien sind, welche Vereinbarungen zwischen Banken und Trackingbetreibern getroffen wurden, ob die Kunden dem Tracking zugestimmt haben, ob es rechtlich zulässig ist und wie groß die tatsächlichen Gefahren sind. Sondern es ging zunächst einmal darum, potenzielle Risiken für Privatsphäre und Sicherheit der Bankkunden aufzuzeigen.

Das Ergebnis ist ernüchternd. Nur fünf der zwölf untersuchten Banken lassen während einer typischen Online-Banking-Sitzung weder auf der Login-Seite noch nach dem Login oder auf der Logout-Seite Tracker dritter Parteien zu. Bei acht Instituten wurden solche Tracker gefunden. Im Einzelnen rufen drei Websites nach erfolgtem Login Dienste von Drittanbietern auf, die Hälfte der Websites überträgt Daten an große Webtracking- und Webanalyse-Anbieter.

Die meisten Tracker entdeckten die Experten auf den Seiten von N26 (früher Number 26). Hier wurden beim oder nach dem Login sowie auf der Logout-Seite Daten unter anderem an Google und Facebook gesendet. Teils führte Software dritter Firmen Java auf den Seiten aus.

Das heißt nicht, dass dabei Kundendaten offen gelegt werden. Sondern es geht darum, Geschäftsprozesse zu optimieren, Kosten zu senken und gegebenenfalls bessere Software-Tools anzubieten. Vielleicht war es deshalb ein Fintech, das in der Untersuchung in besonderem Maße als „Tracking-Sünder" auffiel.

Allerdings bringen die Vorteile, die dieses Vorgehen aus Sicht der Anbieter zweifellos hat, eben auch mit Risiken bezüglich Sicherheit und Datenschutz mit sich. Wenn das Tracking während der eingeloggten Sitzung erfolgt, so die Studie, könnten sich sogar Informationen über den Finanzstatus des Nutzers ableiten lassen. Zumindest geben die eingesetzten technischen Mittel den Drittanbietern die Möglichkeit dazu.

Das Risikopotenzial ist der Untersuchung zufolge unterschiedlich groß, je nachdem, wo die Tracker sitzen und welche Technologien (Cookies, Fingerprinting oder Javascript) im Einsatz sind. Im harmlosesten Fall erhalten Dritte Daten, anhand derer sie identifizieren können, wer bei der jeweiligen Bank ein Konto führt. Im schlimmsten Fall eröffnen Javascript-Technologien Angriffspunkte für Hacker. **Red.**

Banking-Portale mit und ohne Tracking

Kein Tracking	Mindestens ein trackendes Element dritter Firmen
DAB Bank	Comdirect
Hypovereinsbank	Commerzbank
Postbank	Consorsbank
Stadtsparkasse München	Deutsche Bank
Volksbank Mittelhessen	DKB
	ING-Diba
	N26