06.05.2025

Halbjahresbericht des Bundesamtes für Cybersicherheit (BACS)

Erneut verzeichnet das Bundesamt für Cybersicherheit (BACS) mit über 62'000 Meldungen eine deutliche Zunahme an Cybervorfällen im Vergleich zur Vorperiode. Speziell hervorzuheben ist, dass wieder mehr Phishing-Vorfälle via Telefon (Voice-Phishing / Vishing) registriert wurden.

Die Statistik des Bundesamtes für Cybersicherheit (BACS) zeigt, dass Phishing nach wie vor zu den Kernherausforderungen für die Schweizer Wirtschaft und die Bevölkerung gehört. Phishing-Versuche sind mit 12'038 Meldungen, nach Betrug, die am zweithäufigsten gemeldeten Cybervorfälle beim BACS im Jahr 2024. Das ist eine Zunahme von 2'623 Meldungen im Vergleich zum Vorjahr. Nebst dem gängigen Phishing via E-Mail hat im letzten Jahr der Ansatz via Telefon (Voice-Phishing / Vishing) stark zugenommen. Dabei bleiben Phishing-Versuche im Namen von Finanzdienstleistern hoch im Trend. Betrüger haben sich im Jahr 2024 vor allem der, aus den 2010er-Jahren, bekannten Masche «Anrufe von angeblichen Bankmitarbeitenden» bedient. Die Vorgehensweise bleibt gleich, der Vorwand von den Betrügern wurde jedoch angepasst.

Betrüger melden sich beispielsweise als Mitarbeiter der Sicherheitsabteilung eines Finanzinstituts und behaupten, eine betrügerische Zahlung stoppen zu wollen. Perfiderweise wird dem Opfer dabei die effektive Telefonnummer des Finanzinstituts angezeigt. Diese wird mittels «Spoofing» gefälscht. Um eine angeblich betrügerische Abbuchung zu stoppen, liefern die Betrüger direkt eine gefälschte Telefonnummer für einen Anruf bei der angeblichen Polizei mit. Dieser Anruf bei der angeblichen Polizei landet erneut bei den Betrügern. Worauf mittels Anweisungen und gefälschten Links versucht wird, den Opfer Geld abzunehmen und / oder den Zugriff auf deren Konten zu erlangen.

Diese Art des Phishings, also Voice-Phishing oder Vishing, ermöglicht den Betrügern in Echtzeit zu agieren. Dies ist nötig, um in Applikationen zu gelangen, welche durch eine Multi-Faktor-Authentifizierung (MFA) (https://www.ebas.ch/2024/12/multi-faktor-authentifizierung-und-passkeys/) geschützt sind, wie z. B. E-Banking. MFA reduziert das Risiko durch Kompromittierung- kann jedoch durch Social-Engineering-Techniken ausgehebelt werden.

Hier hilft einmal mehr skeptisch zu sein (https://www.ebas.ch/5-aufpassen-und-wachsam-sein/) und zu bedenken, dass Schweizer Banken nie nach Sicherheitsangaben wie Passwörtern, Nummern oder Token von MFA-Applikationen fragen werden.

Weitere Informationen zum Faktor Mensch finden Sie hier (https://www.ebas.ch/2025/04/faktor-mensch-die-groesste-sicherheitsluecke-oder-der-beste-schutz/) .

Den Halbjahresbericht 2024/II (Juli-Dezember) des BACS finden Sie hier (https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/lageberichte/BACS-HJB-2024-2_DE.pdf.download.pdf/BACS-HJB-2024-2_DE.pdf) .