

Social Engineering: (Neue Angriffsmethode richtet sich gegen Firmen)

23.01.2017

Auf einen Blick

In den letzten Tagen wurden der Melde- und Analysestelle Informationssicherung des Bundes (MELANI) mehrere Fälle gemeldet, bei denen Betrüger Firmen anrufen, sich als Bank ausgeben und behaupten, dass am nächsten Tag ein E-Banking-Update durchgeführt würde. Sie verlangen, dass an diesem Termin verschiedene Mitarbeitende der Finanzabteilung anwesend sind. Dies hat den Zweck, das Sicherheitselement «Kollektivunterschrift» auszuhebeln und so eine betrügerische Zahlung auszulösen.

In den letzten Tagen mehren sich Anrufe bei potenziellen Opferfirmen, in denen sich Angreifer als Bankmitarbeitende ausgeben. In vielen Fällen ist die Information, bei welcher Bank die Firma Kunde ist, auf der Firmenwebseite ersichtlich, da dort die Bankverbindung angegeben ist. Die Information kann aber auch im Vorfeld durch die Betrüger mittels Telefonanruf oder E-Mail-Anfrage eruiert werden.

Die Melde- und Analysestelle Informationssicherung MELANI des Bundes hat dazu einen [Newsletter](#) veröffentlicht.

Um sich vor solchen Angriffen zu schützen, empfiehlt MELANI folgende Massnahmen:

- Die Sensibilisierung von Mitarbeitenden bezüglich dieser Vorfälle, insbesondere der Mitarbeitenden in Schlüsselpositionen.
- Sämtliche den Zahlungsverkehr betreffenden Prozesse sollten firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen konsequent eingehalten werden. Finanzinstitute werden Sie weder telefonisch noch schriftlich dazu auffordern, Ihre E-Banking-Zugangsdaten anzugeben.
- Keine seriöse Bank wird Sie auffordern, an Tests von irgendwelchen Sicherheitsupdates mitzuwirken. Die Banken respektive deren IT-Dienstleister verfügen über spezielle Testumgebungen, um Sicherheitsupdates zu prüfen, bevor diese für den Kunden sichtbar werden.
- Installieren Sie niemals Software, wenn Sie telefonisch oder schriftlich dazu aufgefordert werden.
- Erlauben Sie niemals einen Fremdzugriff auf Ihren Computer.
- Reduzieren Sie im Internet publizierte Informationen über Ihr Unternehmen auf das Notwendige. Verzichten Sie wenn möglich auf die namentliche Nennung von Mitarbeitenden sowie auf die Angabe von Bankverbindungen.
- Geben Sie bei zweifelhaften oder ungewöhnlichen Kontaktaufnahmen keine internen Informationen preis.
- Bei ungewöhnlichen Kontaktaufnahmen und Aufforderungen ist es empfehlenswert, innerhalb der Firma Rücksprache zu nehmen, um die Richtigkeit des Auftrags zu verifizieren.
- Falls Sie Opfer von Betrug geworden sind, melden Sie dies via Meldeformular an das Bundesamt für Polizei (fedpol) und erstatten Sie Anzeige bei Ihrer kantonalen Polizeidienststelle.