Social Engineering: Neue Angriffsmethode richtet sich gegen Firmen

In den letzten Tagen wurden der Melde- und Analysestelle Informationssicherung 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 Bankmitarbeiter 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 Anrufer geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll. Um diesen Test durchführen zu können, müssten allerdings alle Mitarbeitende der Finanzabteilung, insbesondere diejenigen, die Unterschriftsberechtigung beim e-Banking haben, anwesend sein. Um Vertrauen zu schaffen, erwähnen die Betrüger zum Teil die Namen von existierenden Mitarbeitenden.

Bei einem weiteren Anruf soll dann ein Fernzugriffstool installiert und dem Anrufer der Zugriff gewährt werden. Dieser gibt vor, anhand einer Testzahlung die Funktionsweise des Systems überprüfen zu wollen. Da das Auslösen von Zahlungen bei Firmen in der Regel durch eine Kollektivunterschrift geschützt ist, fordern die Betrüger die Unterschriftsberechtigten auf, ihre Zugangsdaten anzugeben. In Wirklichkeit geben sie allerdings so die Zahlung frei. In einigen Fällen wird dem Opfer während diesem Vorgang durch die Angreifer ein schwarzer Bildschirm eingeblendet, damit das Opfer die betrügerische Zahlung nicht bemerken kann.

Das Beispiel zeigt, wie aktuell Social Engineering Methoden weiterhin sind. Die Sensibilisierung innerhalb der einzelnen Firmen ist der Schlüssel, solchen Betrugsversuchen wirksam vorzubeugen.

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 resp. 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 Auftrages zu verifizieren.

- Falls Sie Opfer von Betrug geworden sind, melden Sie dies via Meldeformular an das Bundesamt für Polizei fedpol: (https://www.cybercrime.admin.ch/kobik/de/home/meldeformular/melde (https://www.cybercrime.admin.ch/kobik/de/home/meldeformular/meldeformular.html)) und erstatten Sie Anzeige bei Ihrer kantonalen Polizeidienststelle.

Für die IT-Sicherheit in KMUs hat MELANI ein Merkblatt veröffentlicht:

- Merkblatt IT Sicherheit für KMUs: https://www.melani.admin.ch/melani/de/home/dokumentation/checkliste und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html (https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html)

✉ Fachkontakt (mailto:info@melani.admin.ch)

Letzte Änderung 20.01.2017

Social Engineering (/melani/de/home/themen/socialengineering.html)

https://www.melani.admin.ch/content/melani/de/home/dokumentation/newsletter/social-engineering--neue-angriffsmethode-richtet-sich-gegen-firmen.html