

Präventionshinweis zu einer aktuellen Betrugsmasche im Zusammenhang mit dem Online-Banking

Im Rahmen eines aktuell bei der Polizeiinspektion Leer/Emden geführten Ermittlungsverfahrens wurde eine Betrugsmasche bekannt, bei der sich bislang unbekannte Täter unter missbräuchlicher Verwendung des Namens bzw. des Erscheinungsbildes der Deutschen Apotheker- und Ärztebank (ApoBank) Zugang zu den Bankdaten von Geschädigten verschaffen und diese anschließend durch gezielte telefonische Täuschung zur Freigabe von Überweisungen veranlassen.

Nach dem bislang bekannten Vorgehen erhalten die Betroffenen zunächst ein postalisches Schreiben, welches den Eindruck erweckt, von der ApoBank AG zu stammen. Darin werden **die Empfänger unter einem Vorwand aufgefordert, ihr Online-Banking über einen sogenannten „QR-Code“ zu verifizieren**. Andernfalls wird mit Sperrung der digitalen Zugänge gedroht.

In einem weiteren Schritt erfolgt eine telefonische Kontaktaufnahme. Hierbei geben sich die Täter als Bankmitarbeiter aus und behaupten, es seien Unregelmäßigkeiten beziehungsweise unberechtigte Überweisungen auf dem Konto festgestellt worden oder das Online-Banking sei kompromittiert worden.

Hierbei kann auch sogenanntes Call-ID-Spoofing eingesetzt werden. Dabei wird auf dem Display des angerufenen Telefons die tatsächliche Rufnummer der ApoBank angezeigt, obwohl der Anruf tatsächlich von einer anderen Rufnummer ausgeht. Die auf dem Display angezeigte Rufnummer stellt daher keinen sicheren Nachweis für die Identität des Anrufers dar.

Unter dem Vorwand, die angeblich bereits veranlassten Überweisungen zu stornieren beziehungsweise das Konto zu sichern, werden **die Betroffenen anschließend aufgefordert, auf ihrem Mobiltelefon angezeigte Push-Benachrichtigungen oder sonstige Freigabevorgänge zu bestätigen**.

Tatsächlich werden durch diese Bestätigungen nach derzeitiger Erkenntnis Überweisungen freigegeben, die durch die Täter selbst veranlasst wurden. Hierdurch können erhebliche finanzielle Schäden entstehen.

Nach derzeitiger Kenntnis beschränkt sich die Vorgehensweise zudem nicht ausschließlich auf tatsächliche Kunden der ApoBank.

Auch Personen mit anderen Bankverbindungen sollen bereits mit einer entsprechenden Vorgehensweise kontaktiert worden sein.

Besondere Vorsicht ist daher geboten, wenn:

- ein Schreiben oder eine Nachricht vermeintlich von einer Bank zur Verifizierung des Online-Bankings auffordert,
- anschließend ein angeblicher Bankmitarbeiter telefonisch Kontakt aufnimmt,
- auf eine angebliche Kompromittierung des Kontos oder bereits erfolgte Überweisungen hingewiesen wird,
- die betroffene Person zur Bestätigung von Push-Nachrichten oder Transaktionen auf ihrem Mobiltelefon aufgefordert wird,
- oder der Anrufer zur vermeintlichen Stornierung beziehungsweise Sicherung von Zahlungen die Freigabe weiterer Vorgänge verlangt.

Wichtig:

Seitens eines realen Bankmitarbeiters werden sensible Bestätigungen oder die Weitergabe von „PIN“ oder Push-TAN nicht über das Telefon angefordert. Für eine Stornierung oder Änderung benötigt ein realer Bankmitarbeiter derartige Angaben nicht.

Eine auf dem Mobiltelefon angezeigte Transaktion oder Freigabe sollte vor der Bestätigung sorgfältig darauf überprüft werden, welcher Vorgang tatsächlich autorisiert wird. Insbesondere sollte eine Freigabe nicht allein aufgrund einer telefonischen Aufforderung erfolgen.

Bei einem unerwarteten Anruf der eigenen Bank sollte das Gespräch beendet und die Bank ausschließlich über eine bereits bekannte beziehungsweise offiziell recherchierte Telefonnummer selbstständig kontaktiert werden. Die im Rahmen eines solchen Anrufs mitgeteilte Telefonnummer sollte hierfür nicht verwendet werden.

Sollten bereits unberechtigte Transaktionen freigegeben worden sein, sollte unverzüglich die kontoführende Bank kontaktiert und – soweit möglich – eine Rückholung beziehungsweise Sicherung der betroffenen Beträge veranlasst werden. Zudem sollte zeitnah eine Strafanzeige bei der Polizei erstattet werden.