Aktuelle Sicherheitshinweise (Stand: 17.06.2022)

Betrüger nutzen den Krieg in der Ukraine, um Bankkunden zur Weitergabe ihrer Zugangsinformationen zu bewegen.

Die Kontaktaufnahme mit den Bankkunden kann auf verschiedenen Wegen, z.B. E-Mail, SMS oder WhatApp-Nachricht. In den Anschreiben wird mit irgendeiner Begründung mit Bezug zum Ukraine-Konflikt versucht, die Bankkunden zur Weitergabe von Informationen, z.B. Zugangsdaten, Kreditkartennummern, zu bewegen. Ebenso sind gefakte Websites, zum Beispiel mit Spendenaufrufen möglich.

Angeblich hat der Kunde die Zustimmung zur PSD2/EU-Richtlinie noch nicht gegeben.

Betrüger verschicken SMS an potentielle Bankkunden, die den Eindruck erwecken, sie kämen von der Bank. Unter dem Vorwand, es sei dringlich eine Zustimmung notwendig, versuchen Betrüger Zugangsdaten zu Online-Bankkonten zu erlangen. Die dahinter liegende Methode ist klassisches Phishing. Dazu sind auf einer Webseite die Zugangsdaten (BLZ, VR-NetKey und PIN) einzugeben. Darüber hinaus wird zusätzlich das Geburtsdatum und Telefonnummer des Kunden abgefragt.

In betrügerischer Absicht versandte E-Mails, in denen dazu aufgefordert wird, VR SecureGo plus zu bestätigen

Wir warnen im Zusammenhang mit VR SecureGo plus vor E-Mails, in denen die Versender dazu auffordern, die per SMS versandte TAN zum Anzeigen eines Aktivierungscodes für die Geräteaktivierung zu bestätigen. So versuchen die Betrüger, ihr eigenes Mobilgerät für VR SecureGo plus freizuschalten.

Betrugsversuche per Telefonanruf: Betrüger geben sich als Bankmitarbeiter aus

Wir warnen erneut vor Phishing-Versuchen per Telefonanruf, bei denen sich Betrüger als Mitarbeiter der Bank ausgeben. Sie behaupten, die Kunden bei einer vermeintlichen Umstellung des Online-Bankings unterstützen zu wollen. In betrügerischer Absicht versandte E-Mails, die einen QR-Code enthalten, der angeblich die Zustimmung zu neuen AGB ermöglichen soll.