bankenverband

Blog

Betrugsmasche: Manipulation am Telefon

14.04.2022

von

Altmann, Kathleen

Schlagworte

Phishing
Konto
Cyberkriminalität
PIN
Onlinebanking
Cyberattacken
Unternehmen
TAN
Sicherheit
BaFin
Sicherheit Verbraucher

Blog

„Ihr Konto wurde aus Sicherheitsgründen geblockt.“ Oder: „Es gibt ein Problem mit Ihrem Computer.“ Solche oder ähnliche Sätze fallen am Telefon, wenn ein Krimineller versucht, an Ihre persönlichen Daten zu gelangen oder Sie zu einer Zahlung zu veranlassen. Die Betrüger geben sich beispielsweise als Bankangestellte aus, als Mitarbeiter der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), als Ermittler von Europol oder Interpol, oder aber sie behaupten, sie seien vom technischen Support eines Softwareunternehmens. Die Masche ist bekannt: Seriöse Unternehmen dienen als Einstieg in ein Telefonat, das nur darauf abzielt, Ihr Vertrauen zu gewinnen oder Sie unter Druck zu setzen.

Aus „Sicherheitsgründen“ oder um angeblich Ihre Online-Banking-Funktionen wieder herzustellen, sollen dabei Ihre Kontodaten oder andere persönliche Daten, wie Ihre Adresse, „abgeglichen“ werden. Alternativ wird auch „Hilfe“ bei der Umstellung auf ein anderes TAN-Verfahren angeboten. In einigen Fällen wird der Kriminelle versuchen, über eine Fernwartungssoftware Zugang zu Ihrem Computer zu erhalten. Ziel ist es, Sie so zu manipulieren, dass Sie unbeabsichtigt eine Zahlung per TAN freigeben.

Manipulierte Telefonnummern

Auf dem Display Ihres Telefons erscheint vermeintlich die Nummer Ihrer Bank oder des Kundenservices des Softwareunternehmens. Tatsächlich ist diese Rufnummernanzeige manipuliert, um Sie zu täuschen. Lassen Sie sich von dieser Telefonnummer nicht in die Irre führen. Fragen Sie den Anrufer nach seinem Namen, sagen Sie ihm, dass Sie sich melden werden, und legen Sie vorsichtshalber auf!

Recherchieren Sie jetzt unabhängig: Schauen Sie auf der richtigen Unternehmenswebseite, fragen Sie die Auskunft oder suchen Sie im Telefonbuch nach dem Anrufer. Nutzen Sie für den Rückruf auf keinen Fall die am Telefon genannte oder die im Display angezeigte Telefonnummer.

No-Go: Fremde auf Ihren Rechner zugreifen lassen

Spätestens, wenn der Anrufer einen vermeintlichen Fehler auf Ihrem Computer beheben oder das geblockte Konto „entsperren“ will und Ihnen dabei ankündigt, dass er auf Ihren Rechner von extern zugreifen muss, sollten bei Ihnen alle Alarmglocken schrillen! Vordergründig geht es um Hilfe, tatsächlich aber lauert dahinter die Übernahme Ihres Rechners.

Besonders vertrauenswürdig wirkt die Betrugsmethode, wenn Sie bereits einige Tage zuvor eine Mail mit einem Link, angeblich von Ihrer Bank, erhalten haben (Phishing-Mail). Ruft Sie nun der angebliche Bankmitarbeiter an, erzeugt dieses Zusammenspiel von Mail und Telefonat bei Ihnen den Eindruck

einer gewissen Seriosität. Sie sind eher geneigt, dem Anrufer zu vertrauen.

Im Laufe des Gesprächs werden Sie aufgefordert, den Link aus der Mail anzuklicken. Eine beispielhafte Redewendung hierfür ist: „Sie können natürlich auch zu uns in die Filiale kommen. Aber wenn Sie möchten, kann ich auch gleich von hier den Fehler korrigieren.“

Auch hier gilt: Folgen Sie keinem Link und laden Sie sich kein Programm herunter, selbst wenn der Anrufer auf Sie einen sehr sympathischen und vertrauenserweckenden Eindruck macht.

Nicht unter Druck setzen lassen

Egal, welche Szenarien der Anrufer aufzeigt: Wichtig ist, dass Sie ruhig und besonnen bleiben und sich nicht unter Druck setzen lassen. Der Kriminelle wird möglicherweise alle Register ziehen: Er könnte beispielsweise behaupten, dass Ihnen eine Kontosperre drohe, dass Sie finanzielle Einbußen erleiden würden. Aber auch wenn er Ihnen mit einem Rechtsanwalt oder einem Inkassobüro droht: Lassen Sie sich nicht einschüchtern!

Er könnte aber genauso gut an Ihr Verantwortungsgefühl appellieren, indem er Sie um Mithilfe bei der Verbrechensbekämpfung oder Ähnliches bittet.

Auch eine sehr freundliche und vertrauensvolle Atmosphäre sollte Sie nicht verleiten, aktiv zu werden. Ziel ist zu jeder Zeit, Sie zum Handeln zu bewegen: dem Link zu folgen, Ihre Daten einzugeben, eine Fernwartungssoftware herunterzuladen oder auf anderem Wege an Ihre persönlichen Daten zu gelangen. Legen Sie im Zweifel einfach auf!

Top secret: Persönliche Daten

Allgemein gilt: Gehen Sie verantwortungsvoll mit all Ihren persönlichen Daten um. Dazu gehören neben Ihren Kartendaten, PINs und TANs auch Ihre Adresse, Ihre Telefonnummern oder Ihr Geburtsdatum. Überlegen Sie stets, ob diese Informationen für den beabsichtigten Vorgang überhaupt benötigt werden.

Strafanzeige erstatten

Wichtig: Wenden Sie sich bei jeglichem Missbrauch Ihrer Bankdaten – und auch schon bei einem Verdacht – umgehend an Ihre Bank. Kontaktieren Sie zudem die Polizei und erstatten Sie Strafanzeige. Nur wenn der Betrug angezeigt wurde, kann er auch strafrechtlich verfolgt und den Kriminellen das Handwerk gelegt werden.