Medieninformation
Nr. 378

Ihr Ansprechpartner
Andrzej Rydzik

Durchwahl
Telefon +49 371 387-2020
Telefax +49 371 387-2044

medien.pd-c@
polizei.sachsen.de

Chemnitz, 26. August 2022

Direktionsbereich

Polizei warnt vor neuer Betrugsmasche namens „Vishing“

(2968) Bundesweit macht aktuell ein neues Betrugsphänomen die Runde. „Vishing“ – ist eine Abwandlung vom bereits bekannten „Phishing“, wobei das V für „voice“ steht und ein Telefonat zum Ausdruck bringt, womit die Betrugsmasche ihren Lauf nimmt.

Die Masche: Die Opfer werden telefonisch von einem angeblichen Mitarbeiter der Hausbank kontaktiert. Durch geschickte Gesprächsführung bringt die Täterschaft dabei das betreffende Geldinstitut in kürzester Zeit in Erfahrung. Den Opfern wird erklärt, dass es zu unberechtigten Abhebeversuchen mit einer kopierten Girocard beziehungsweise EC-Karte kam oder der Bank eine Überweisung für das Ausland vorläge. Auch andere Varianten sind möglich. Situationsbedingt erfolgt teilweise eine vorgetäuschte Vermittlung an die fiktive Sicherheitsabteilung oder die angebliche Polizei, sodass ein Mittäter das Gespräch fortführt. Haben die Täter ihr Opfer an der sprichwörtlichen Angel, legen sie los. Sie erzählen den Angerufenen, dass vorsorglich das Konto gesperrt worden sei und man unter anderem zur Spurensicherung die echte Bankkarte sowie die PIN benötige. Noch während des minutenlangen Gesprächs erscheint ein angekündigter Bote der angeblichen Bank und lässt sich die Karte aushändigen. Anschließend beendet der Anrufer das Telefonat mit der Bemerkung, es sei alles in Ordnung, der Kunde werde eine neue Bankkarte erhalten. Eine erste Verfügung mit der erlangten Bankkarte erfolgt anschließend meist umgehend in Tatortnähe, sodass selbst bei zeitnaher Kartensperrung ein Schadenseintritt unvermeidbar ist. Bei nicht erfolgter Sperrung erfolgen binnen kurzer Zeit weitere Abhebungen.

Die Begehungsweise der Täter kann aber auch variieren. Ebenfalls unter dem Vorwand, die Sicherheitsabteilung der Hausbank habe einen Missbrauch festgestellt, werden telefonisch vom Opfer die Zugangsdaten zum Onlinebanking und eine TAN in Erfahrung gebracht. Am Anfang steht hier jedoch eine klassische Phishing-Mail: Der Empfänger der Nachricht wird zur Preisgabe seiner Kontodaten veranlasst und erhält in der Folge einen vermeintlich von der Hausbank stammenden Anruf. Die Rufnummer wird durch die Täterschaft unter Nutzung des Call-ID-Spoofings, also der zielgerichteten Manipulation der eigenen Rufnummer, generiert. Den Opfern wird somit die tatsächliche oder eine ähnliche Rufnummer der Hausbank angezeigt. Mit den erlangten Informationen aus der Phishing-Mail und den telefonisch übermittelten Daten legen die Täter eine virtuelle Debitkarte auf ihrem Smartphone an. Auf diese Weise wird das

Polizeidirektion Chemnitz
Hartmannstraße 24
09113 Chemnitz

www.polizei.sachsen.de

Verkehrsanbindung:
Zu erreichen mit den Buslinien 21,32
H: Richard-Hartmann-Platz

Behindertenparkplätze:
Promenadenstraße

Mobiltelefon zur Geldbörse, indem es einfach vor das Kassenterminal gehalten wird. Die PIN zur Karte wird in diesem Fall nicht benötigt, weil das Mobiltelefon bekanntlich nach einer Freigabe durch Wischgestik, PIN-Eingabe, Fingerprint oder Irisscanner verlangt. Somit entfällt die bei Vorlage der physischen Karte verlangte PIN-Eingabe und die Täter können freizügig auf Einkaufstour gehen. Innerhalb kürzester Zeit werden auf diese Weise Umsätze im mittleren vierstelligen Bereich realisiert, gern durch Erwerb von leicht zu veräußernden Guthabenkarten.

Die Täter haben durch den Online-Zugriff auf das Geschädigtenkonto Kenntnis vom vorhandenen Guthaben und räumen es sprichwörtlich leer. Der Schaden läuft zu 100 Prozent zu Lasten des Kontoinhabers. Die kontoführenden Institute lehnen aufgrund der Herausgabe der sensiblen Daten Schadensersatzleistungen generell ab.

Einer der ersten Vishing-Fälle im Zuständigkeitsbereich der Polizeidirektion Chemnitz ereignete sich am **12.08.2022 in Schwarzenberg, OT Crandorf**. Dort hatte ein Mann einen Anruf einer vermeintlichen Mitarbeiterin seines Kreditinstituts erhalten. Sie hatte ihm mitgeteilt, dass es bankintern zu Problemen gekommen sei und man aus diesem Grund die Kunden nun telefonisch kontaktiere. Dass der Angerufene das Push-TAN Verfahren auf seinem Smartphone nutzt und auch die Kontonummer des Mannes war für die Anruferin schnell in Erfahrung gebracht. Sie teilte dem Betrugsopfer mit, dass er eine Überweisung zur Probe ausführen müsse. Im weiteren Verlauf des Telefonats wurde der Mann dazu bewegt, 3.000 Euro auf ein fremdes Konto zu überweisen.

In diesem Zusammenhang warnt die Polizei:

- **Geben Sie am Telefon keine persönlichen Informationen** weiter **– keine Telefonnummern und Adressen, Kontodaten, Bankleitzahlen oder Kreditkartennummern!** Firmen bzw. Banken, bei welchen Sie tatsächlich Kunde sind, haben Ihre Daten vorliegen und müssen diese nicht erfragen.

- **Seien Sie skeptisch am Telefon, wenn es um finanzielle Angelegenheiten geht und hinterfragen Sie im Zweifel die geschilderten Begebenheiten kritisch!**

- **Wenden Sie sich an Ihre örtliche Polizeidienststelle, wenn Sie verdächtige Anrufe erhalten und erstatten Sie unbedingt Anzeige!** Dies hilft den Strafverfolgungsbehörden bei der Detektion neuer Phänomene und der Aufklärung der dahinter stehenden Strukturen. (Ry/rp)