2FA: Die Bestätigung in zwei Schritten

Schon mehrfach haben wir im Newsletter über die sogenannte Zwei-Faktor-Authentifizierung oder “Bestätigung in zwei Schritten” gesprochen.
Die **Zwei-Faktor-Authentifizierung (oft auch als “2FA” abgekürzt)** ist ein Sicherheitsverfahren, bei dem man sich nicht nur mit einem Passwort anmeldet, sondern auch einen zweiten Bestätigungsschritt durchführt, z.B. mit einem Code, der auf das Handy geschickt wird. Dieser zweite Schritt erfolgt immer über einen zweiten “Kommunikationskanal”, der ein anderer Kanal ist, als der Kanal, auf dem das eigentliche Passwort eingegeben wurde. Es gibt verschiedene Kanäle, zum Beispiel: E-Mail, SMS, Anruf, App, Browser, Briefpost. Das macht es schwieriger für Unbefugte, auf unsere Benutzerkonten zuzugreifen, weil sie neben dem Passwort auch diesen zusätzlichen Code aus dem zweiten Kommunikationskanal benötigen. Das erhöht die Sicherheit von Online-Konten erheblich! Denn selbst wenn Hacker uns erfolgreich angreifen konnten, haben sie dann nur Zugriff auf einen dieser Kanäle (zum Beispiel: E-Mail-Adresse). Sobald die Zusatzabfrage des 2FA auf einem anderen zweiten Kanal erfolgt (zum Beispiel: SMS), werden die Hacker bloßgestellt.
Hier können Sie unseren letzten Beitrag dazu im Archiv nachlesen.
Die Zwei-Faktor-Authentifizierung wird mittlerweile von vielen Online-Diensten eingesetzt, darunter Google, Facebook, Apple, PayPal, beim Online-Banking etc. Ein ganz klassisches Beispiel ist die **TAN beim Online-Banking**. Möchte man eine Überweisung tätigen, so schickt uns die Bank zunächst eine TAN, die entweder auf dem Smartphone oder mit einem speziellen TAN-Generator erstellt wird. Erst danach kann die Überweisung ausgeführt werden. Das bedeutet, selbst wenn Kriminelle das Passwort von unserem Online-Banking-Zugang kennen würden, könnten sie dennoch keine Überweisung durchführen, da sie dafür auch das Gerät brauchen, auf dem die TAN angezeigt wird.
Salopp könnte man sagen, der zweite Schritt der Bestätigung ist immer eine **Rückversicherung**. Und genau diese Rückversicherung lässt sich auch auf viele andere Szenarien im Alltag übertragen, um Betrugsversuche zu erkennen. Einige Beispiele:

1. Enkeltrick

Vor einiger Zeit haben wir über den Fall des Enkeltricks per WhatsApp und SMS berichtet. Betrüger melden sich per Textnachricht und geben sich als das eigene Kind aus. Sie schreiben: *“Hallo Mama, ich habe eine neue Handynummer, bitte speichere die Nummer ab.”* Tut man dies, so entsteht eine Unterhaltung, in der schnell um Geld gebeten wird. Doch bevor man wirklich die Nummer abspeichert und anfängt zu schreiben, sollte der erste Schritt die Rückversicherung sein. Nämlich ein Anruf oder eine Nachricht an die alte, echte Nummer des eigenen

Kindes. „Stimmt es, dass du eine neue Handynummer hast?“ So lässt sich der Betrug sofort enttarnen.
Tipp: Lesen Sie hier unseren ausführlichen Beitrag zum Enkeltrick bei WhatsApp.

2. PayPal-Anruf
Ein anderes Beispiel: Es gibt zur Zeit Fälle von gefälschten Anrufen, die angeblich von PayPal stammen. Eine Computerstimme behauptet, es sei Geld von Unbefugten von Ihrem PayPal-Konto abgebucht worden. Man solle nun verschiedene Dinge tun um diese Abbuchung zu verhindern bzw. rückgängig zu machen. Statt diesen Anweisungen sofort zu folgen, sollte der erste Schritt der Rückversicherung immer sein: melden Sie sich in Ihrem PayPal-Konto an und kontrollieren Sie dort, ob es tatsächlich eine Abbuchung gegeben hat.
Lesen Sie hier unseren ausführlichen Beitrag zu diesem Fall.

3. Stimmen-Imitation
Mit neuer Technologie ist es mittlerweile sogar möglich, Stimmen sehr gut nachzumachen. Auch das machen sich Betrüger zu Nutze. Es gibt bereits Fälle in denen Kriminelle mit der gefälschten Stimme der Kinder bei den Eltern anrufen und per Telefon eine Notsituation beschreiben, mit der dringenden Bitte um einen hohen Geldbetrag. Auch in solchen Fällen gilt: wenn Sie einen Anruf dieser Art erhalten, bleiben Sie besonnen und rufen Sie auf jeden Fall zuerst Ihre Kinder auf deren Telefonnummer zurück, bevor Sie handeln.

4. Mail der Bank
Natürlich sind auch noch ganz klassische Spam-E-Mails im Umlauf, wie man sie seit Jahren kennt. Diese Arbeiten meist mit so genannten Phishing-Versuchen. Das heißt, in der E-Mail, die aussieht, als sei sie von Ihrer Bank, wird behauptet, es gäbe ein Problem mit Ihrem Zugang und Sie müssten sich daher erneut anmelden. In der Regel sind solche E-Mails immer ein Betrugsversuch, da die Bank niemals solche E-Mails verschickt. Wenn Sie sich trotzdem unsicher sind, so kontaktieren Sie immer zuerst den Kundenberater Ihrer Bank, bevor Sie tätig werden und irgendwo Ihr Passwort eingeben.

Tipp: Familienkennwort
Einige Experten raten übrigens dazu, ein eigenes internes geheimes “Familienkennwort” einzuführen. Das ist ein Geheimwort, das nur die eigene Familie kennt. Dieses Geheimwort ist kein klassisches Passwort, das irgendwo eingetragen wird, sondern es ist ein Passwort, das alle Familienmitglieder im Gedächtnis haben und dadurch im Gespräch die eigene Identität bestätigen können. Bei zweifelhaften Anrufen, SMS oder WhatsApp-Nachrichten können Sie dieses Kennwort in der Unterhaltung quasi zwischen den Zeilen abfragen, um ganz sicher zu gehen, dass Sie es tatsächlich mit Ihren Familienmitgliedern zu tun haben.

Quelle: https://levato.de/die-bestaetigung-in-zwei-schritten/?utm_source=mailpoet&utm_medium=email&utm_campaign=2FA+-+Diese+Abk%C3%BCrzung+verbessert+die+Sicherheit