**Hacker machen keine Ferien!**

Immer mehr Menschen arbeiten im Internet und mithilfe einer Cloud. Dabei wird jedoch häufig die Sicherheit vernachlässigt. Arbeitsschritte werden an die digitale Arbeit angepasst, die Sicherheitseinstellungen jedoch nicht. Dadurch ist es für Betrüger ein Leichtes, durch Pishing-Attacken an Benutzernamen und Passwörter zu kommen.

Die bevorstehende Sommerzeit bringt weitere Risiken mit sich. In der Ferienzeit wird nicht nur Pause von der Arbeit gemacht, sondern oftmals auch von der Achtsamkeit vor solchen Angriffen. Doch Hacker machen keine Ferien!

Abhilfe schaffen soll die Multifaktor-Authentifizierung (MFA), ein Begriff, der im Zusammenhang mit Sicherheit immer wieder auftaucht. Doch was genau bedeutet er und warum ist er so bedeutsam?

Um die Hintergründe beleuchten zu können, ist es zunächst wichtig, den Begriff an sich zu verstehen.

**Was ist eine MFA?**

Wie diese Wortkonstellation schon sagt, beschreibt eine MFA die Authentifizierung, also die **Identifikation** einer Person, mittels **mehrerer** **Faktoren**. Um auf einen bestimmten Account zugreifen zu können, benötigt man nicht mehr nur einen Benutzernamen und ein Passwort, sondern eine Kombination aus mehreren Identifizierungs-Faktoren.

In Fachkreisen werden diese Faktoren in drei verschiedene Kategorien unterteilt:

a) Wissen: Passwörter, PIN, …

b) Besitz: Karten, Token, Mobiltelefon, …

c) Biometrische Daten: Fingerabdruck, Stimme, Gesichtserkennung, …

**Anwendungs-Beispiele**

* Ein Beispiel für die Faktoren „Wissen“ und „Biometrische Daten“ ist etwa die Kombination aus Passwort und Fingerabdruck. Nach Eingabe des Passwortes erscheint automatisch ein Feld, welches einen hinterlegten Fingerabdruck verlangt. Anschließend wird der Account geöffnet.
* Ein Beispiel für die Kombination der Faktoren Wissen und Besitz ist der Versand eines Authentifizierungs-Codes, nach der Eingabe eines Passwortes. Der Nutzer muss den erhaltenen Code (via SMS oder E-Mail), in ein dafür vorgesehenes Feld eingeben, um den Account zu erreichen. Das Passwort entspricht hier dem Faktor „Wissen“, während der Code, welcher den Besitz eines mobilen Gerätes voraussetzt, dem Faktor „Besitz“ entspricht.

**Warum ist eine Identifizierung mithilfe mehrerer Faktoren nötig?**

Durch den Wechsel in die Cloud und die dabei vergessene Aktualisierung der Sicherheitseinstellungen, kommen Hacker leichter an Benutzernamen und Passwörter.

Und genau hier kommt den Nutzern die MFA zugute. Gelingt es einem Hacker, durch den Diebstahl der Zugangsdaten, den ersten Anmeldeschritt zu überwinden, wird er im nächsten Schritt vor beinahe unüberwindbare Sicherheitsmauern gestellt. Wird von Eindringling nun ein Identifizierungs-Code oder ein Fingerabdruck verlangt, kann er den Account trotz richtiger Daten nicht erreichen.

**Wie kann ich diese Technologie nutzen?**

Als Partner von Microsoft bietet Ihnen KONVERTO verschiedene Sicherheitslösungen und steht Ihnen als Experten auf diesem Gebiet beratend zur Seite zu stehen.

Unter unserer kostenlosen Nummer 800 031 031 erhalten Sie alle wichtigen Informationen. Sie erreichen uns auch unter info(at)konverto.eu.

**Wie kann ich mich und meine Mitarbeiter angemessen vorbereiten?**

Rund 80% der Vorfälle werden durch Fehlverhalten von Nutzern, aufgrund von Unachtsamkeit, ausgelöst. Daher ist es unerlässlich ein Sicherheitsbewusstsein für das Unternehmen und dessen Mitarbeiter zu schaffen. KONVERTO bietet gezielte Awareness-Trainings an, um Sie auf den Ernstfall vorzubereiten.

**Wie sieht die Zukunft der Authentifizierung aus?**

Seit mehreren Jahren wird die MFA verwendet. Die genannten Faktoren werden jedoch nicht nur in Kombination mit Passwörtern verwendet, sondern sind auch im Einzelnen bereits im Einsatz. Dies spiegelt auch der Trend hin zur „Passwordless Authentification“ wider, also zur Identifizierung, ganz ohne Passwörter, die man ohnehin immer wieder vergisst und sehr anfällig für Pishing-Attacken sind.