Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) bezeichnet ein IT-Sicherheitsverfahren, mit dem Nutzer bei Anmeldeprozessen ihre Identität nachweisen müssen. Unter anderem kommt das Verfahren beim Online Banking zum Einsatz.

Wissen, Besitz, Inhärenz

Wie der Name bereits verrät, werden bei der Zwei-Faktor-Authentifizierung beim Nutzer zwei unterschiedliche und unabhängige Faktoren abgefragt. Insgesamt gibt es drei Faktoren, die zur Authentifizierung eingesetzt werden können:

- eine PIN oder ein Passwort (Faktor „Wissen“)
- eine Bankkarte oder ein Handy, das SMS empfängt (Faktor „Besitz“)
- biometrische Merkmale wie z. B. ein Fingerabdruck (Faktor „Inhärenz“)

Nur wenn zwei dieser drei Merkmale zusammen zum Einsatz kommen und beide korrekt sind, hat die Authentifizierung Erfolg. Fehlt hingegen ein Faktor oder ist eine Komponente falsch, kann die Berechtigung nicht erteilt werden. Folglich wird dem Nutzer der Zugriff verweigert.

Mehr Sicherheit beim digitalen Bezahlen

Die Zugriffsmethode über zwei Faktoren wird bereits seit langer Zeit beim Betreten von sicherheitsrelevanten Gebäuden oder Räumlichkeiten über einen Zugangscode sowie einen zusätzlichen Fingerabdruck angewendet. Neuerdings soll mithilfe des Verfahrens aber vor allem das Bezahlen im Internet sicherer werden. Demnach ist es für die Banken verpflichtend, zwei der oben genannten drei Merkmale für die Authentifizierung ihrer Kunden einzusetzen. Wer also eine Online-Überweisung tätigt oder online mit Kreditkarte bezahlt, muss sich mithilfe von zwei Faktoren als die Person ausweisen, der das Konto gehört. Das geschieht meist mit einer PIN oder einem Passwort in Verbindung mit einer TAN. Weil es für Kriminelle bei einer Zwei-Faktor-Authentifizierung nicht ausreicht, das Zugangsgerät des Opfers zu stehlen, können Identitätsdiebstahl, Phishing-Angriffe und andere Online-Betrugsversuchen reduziert werden.

Siehe auch:
TAN
Cybercrime
Phishing

Zurück

© Verlag Deutsche Polizeiliteratur