Es sind Zahlen, die hängen bleiben.

11,7 Millionen Nutzerkonten könnten betroffen sein – eine Dimension, die man nicht einfach mit einem Schulterzucken abtut. Das französische Innenministerium bestätigte am 21. April 2026 einen Sicherheitsvorfall beim Portal der Agence nationale des titres sécurisés, kurz ANTS. Eine Plattform, die für viele längst so selbstverständlich ist wie der Gang zum Amt früher: Personalausweis, Führerschein, Fahrzeugpapiere – alles digital organisiert.

Und nun das.

Der Vorfall selbst wurde datiert auf den 15. April. Was zunächst diffus klang, bekam binnen 24 Stunden Kontur. Betroffen seien vor allem Identifikationsdaten: Namen, E-Mail-Adressen, Geburtsdaten, Login-Kennungen. In einigen Fällen auch Postanschriften oder Telefonnummern. Sensible Dokumente? Biometrische Daten? Fehlanzeige – zumindest nach aktuellem Stand. Die Behörden bemühen sich sichtbar, die Lage zu beruhigen.

Doch wer schon einmal eine Phishing-Mail im Posteingang hatte, ahnt, wo das Problem liegt.

Denn genau hier beginnt die eigentliche Gefahr. Nicht der direkte Zugriff auf Konten, sondern das, was Kriminelle daraus machen. Täuschend echte Nachrichten, sauber personalisiert, mit genau den Details, die Vertrauen schaffen. Ein falscher Klick – und zack, schon steckt man drin im Schlamassel. Die Commission nationale de l’informatique et des libertés warnt seit Jahren vor genau solchen Szenarien.

Parallel läuft die Aufarbeitung auf Hochtouren.

Die Datenschutzbehörde ist informiert, die Pariser Staatsanwaltschaft eingeschaltet, spezialisierte Cyber-Ermittler arbeiten am Fall. Zusätzlich prüft die Verwaltung intern, wer wann was wusste – und ob irgendwo geschlampt wurde. Hinter den Kulissen dürfte es ziemlich knirschen.

Und politisch?

Heikel, keine Frage. Wenn ein zentrales staatliches Portal in dieser Größenordnung betroffen ist, kratzt das am Fundament der digitalen Verwaltung. Bürger sollen Vertrauen haben, ihre Daten online anzugeben – und genau dieses Vertrauen gerät ins Rutschen, sobald solche Meldungen Schlagzeilen machen.

Das Ministerium setzt daher auf eine klare Botschaft: keine Panik. Kein unmittelbarer

Handlungsdruck. Aber erhöhte Wachsamkeit.

Heißt im Alltag: keine dubiosen Links anklicken, keine sensiblen Daten per Mail preisgeben, im Zweifel direkt über die offizielle Website gehen. Und ja, ein neues Passwort schadet nie – am besten eins, das man nicht schon dreimal verwendet hat.

Klingt banal, ist aber entscheidend.

Denn am Ende zeigt dieser Fall vor allem eines: Digitalisierung macht vieles einfacher – aber eben auch verletzbarer. Und Sicherheit ist kein Zustand, sondern ein Dauerlauf.

Oder, um es weniger geschniegelt zu sagen: Ganz ohne Risiko läuft der Laden halt nicht.

Autor: Christine Macha