NACHRICHTEN AG

27. Mai 2025

Sicherheits-Alarm! Überprüfen Sie jetzt Ihre E-Mail auf Datenlecks!

Erfahren Sie, wie "Have I Been Pwned?" neue Funktionen bietet, um Ihre E-Mail-Sicherheit zu überprüfen und zu verbessern.

Australien - Die Popularität von Online-Plattformen hat die Notwendigkeit erhöht, persönliche Daten, insbesondere Passwörter, zu schützen. Ein wichtiges Werkzeug zur Überprüfung der eigenen Sicherheitslage ist die Website „Have I Been Pwned?“ (HIBP), die kürzlich ein neues Design und neue Funktionen vorgestellt hat. Laut **tz.de** wird die Seite von dem australischen Cybersecurity-Experten Troy Hunt betrieben und erlaubt Nutzern, ihre E-Mail-Adressen einzugeben, um zu prüfen, ob ihre Daten in bekannten Datenlecks kompromittiert wurden.

Ein zentrales Merkmal von HIBP ist die Benutzerfreundlichkeit: Ergebnisse sind meist innerhalb von 30 Sekunden verfügbar. Entdeckt ein Nutzer keine kompromittierten Daten, wird dies

durch einen grünen Rahmen und Konfetti gefeiert. Im Falle eines Treffers wird der Nutzer jedoch durch einen roten Rahmen gewarnt. Zudem bietet die neue Zeitleiste den Monat und das Jahr der jeweiligen Sicherheitsvorfälle an, was es einfacher macht, den Zeitpunkt des Datenlecks nachzuvollziehen **dmarcreport.com**.

Regelmäßige Überprüfungen empfohlen

Die Wichtigkeit regelmäßiger Überprüfungen wird unterstrichen: Ein Nutzer fand heraus, dass seine Anmeldeinformationen innerhalb von nur sechs Monaten drei Mal betroffen waren. Daher empfiehlt es sich, seine E-Mail-Adresse regelmäßig bei HIBP zu prüfen. Nach einer negativen Abfrage sollte allerdings keine Entwarnung gegeben werden, da Datenlecks häufig auftreten können. Die Datenbank von HIBP umfasst mittlerweile über 12 Milliarden Datensätze aus verschiedenen Leaks und wird regelmäßig aktualisiert **tz.de**.

Bei einem positiven Treffer rät HIBP, betroffene Passwörter umgehend durch sichere, individuelle Passwörter zu ersetzen. Die Nutzung von Passwortmanagern wird empfohlen, um die Verwaltung komplexer Passwörter zu erleichtern. Auch der Identity Leak Checker des Hasso-Plattner-Instituts wird als nützliches zusätzliches Werkzeug hervorgehoben.

Zwei-Faktor-Authentifizierung als Sicherheitsmaßnahme

Um die Sicherheit weiter zu erhöhen, verdienen Methoden wie die Zwei-Faktor-Authentifizierung (2FA) besondere Beachtung. Die **Bundesstelle für Sicherheit in der Informationstechnik (BSI)** empfiehlt, 2FA nicht zu deaktivieren, um Identitätsdiebstahl und Datenverlust zu vermeiden. Diese Methode ergänzt das Passwort um einen zusätzlichen Faktor, der zur Verifikation erforderlich ist und kann in verschiedenen Formen auftreten, z.B. durch biometrische

Daten oder Hardwaretokens.

Die Verwendung von 2FA ist besonders wichtig, da über 80 % der Datenpannen durch schwache oder gestohlene Passwörter verursacht werden. Dabei sind externe Systeme oft für die Überprüfung eines zweiten Faktors verantwortlich, was die Sicherheit signifikant erhöht **dmarcreport.com**.

Zusammenfassend lässt sich sagen, dass eine proaktive Herangehensweise an Datensicherheit entscheidend ist. Die Nutzung von Tools wie HIBP sowie die Implementierung von Zwei-Faktor-Authentifizierung können entscheidend zur Sicherheit im digitalen Raum beitragen.

Details	
Vorfall	Cyberkriminalität
Ort	Australien
Quellen	• **www.tz.de** • **dmarcreport.com** • **www.bsi.bund.de**