NACHRICHTEN AG

05. Juni 2025

Achtung! 184 Millionen Daten geleakt – So schützen Sie sich jetzt!

Im Juni 2025 wurden 184 Millionen Zugangsdaten in einer unsicheren Datenbank veröffentlicht. Experten raten zu Sicherheitsmaßnahmen gegen Phishing und Datenmissbrauch.

Deutschland - Am 5. Juni 2025 wurden alarmierende Sicherheitsbedrohungen in Form eines massiven Datenlecks bekannt, bei dem über 184 Millionen Zugangsdaten veröffentlicht wurden. Diese Daten, die aus einer ungesicherten Datenbank stammen, umfassen unverschlüsselte Passwörter und E-Mail-Adressen, die für Benutzer mancher der größten Online-Dienste wie Google, PayPal und Netflix zu einem potenziellen Sicherheitsrisiko werden könnten. Laut den Angaben von **Ruhr24** hat die Datenbank ein Volumen von 47 Gigabyte.

Insgesamt wurden 184.162.718 Datensätze registriert, die

vermutlich durch Infostealer-Malware gesammelt wurden. Diese Malware ist dafür bekannt, sensible Informationen aus Browsern und Anwendungen auszuspähen und wird häufig durch Phishing-E-Mails oder bösartige Websites verbreitet, wie **BornCity** berichtet. Die Datenbank, die von Sicherheitsforscher Jeremiah Fowler entdeckt wurde, enthielt neben Zugangsdaten auch Bankinformationen und Kryptowallet-Zugänge sowie .gov-E-Mail-Adressen aus 29 verschiedenen Ländern, darunter Deutschland.

Warnungen und Sicherheitsempfehlungen

Diese massiven Datenlecks haben zahlreiche Sicherheitsbedenken hervorgerufen. Experten empfehlen betroffenen Nutzern, ihre Passwörter umgehend zu ändern und vorzugsweise einzigartige Passwörter für jeden Dienst zu verwenden. Darüber hinaus sollten Nutzer folgende Sicherheitsmaßnahmen in Betracht ziehen:

- Passwortmanager nutzen
- Zwei-Faktor-Authentifizierung aktivieren
- E-Mail-Check bei HaveIBeenPwned durchführen
- Kontoüberwachung aktivieren
- Antivirus-Software nutzen

Langfristige Schutzmaßnahmen, wie die Nutzung von VPN-Diensten und die regelmäßige Aktualisierung von Antiviren-Software, werden ebenfalls empfohlen. Die gesamte Liste der betroffenen Dienste kann auf Plattformen wie HaveIBeenPwned eingesehen werden. Zudem ist es wichtig, sensible E-Mails zu löschen und kontinuierlich über den Status der eigenen Sicherheitsvorkehrungen informiert zu bleiben, um sich gegen potenzielle Phishing-Angriffe zu wappnen.

Die Rolle der Infostealer-Malware

Die Bedrohung durch Infostealer ist im Jahr 2025 besonders ausgeprägt. Laut Berichten von **RedGuard**, gehörten im vergangenen Jahr über 3,2 Milliarden Zugangsdaten zu den

gravierendsten Cyber-Bedrohungen, wobei 75% dieser Leaks durch Infostealer verursacht wurden. Es wird darauf hingewiesen, dass die Infostealer in der Lage sind, Login-Daten, Browser-Cookies und Kreditkarteninformationen zu stehlen. Dies bringt nicht nur Privatpersonen, sondern auch Unternehmen in erhebliche Gefahr.

In einem sich ständig verändernden digitalen Umfeld ist es unerlässlich, sich den Risiken bewusst zu sein und proaktive Sicherheitsmaßnahmen zu ergreifen. Die Sensibilisierung für solche Bedrohungen ist entscheidend, und das Einhalten der empfohlenen Sicherheitsprotokolle sollte für jeden Nutzer Priorität haben, um sich gegen Cyberangriffe zu schützen.

Details	
Vorfall	Cyberkriminalität
Ursache	Infostealer-Malware
Ort	Deutschland
Quellen	• **www.ruhr24.de** • **www.borncity.com** • **www.redguard.ch**