NACHRICHTEN AG

03. Mai 2025

Datenleck im Darknet: 241 Abgeordnete in Gefahr – Schock für Sachsen!

Im Darknet wurden Logindaten von 241 deutschen Landtagsabgeordneten gefunden, darunter auch sächsische Abgeordnete. Cybersecurity-Experten warnen vor Risiken.

Sachsen-Anhalt, Deutschland - Ein alarmierender Vorfall im Bereich der Datensicherheit hat in Deutschland für Schlagzeilen gesorgt. Ein Schweizer IT-Unternehmen, Proton, hat im Darknet Login-Daten von 241 deutschen Landtagsabgeordneten entdeckt. Besorgniserregend ist, dass teilweise sogar die Passwörter offen lesbar sind. Betroffene Abgeordnete nutzen ihre offiziellen E-Mail-Adressen für Konten auf Plattformen wie Dropbox, LinkedIn und Adobe, wodurch die Gefahr einer Missbrauchs erheblich steigt.

Die Bundesländer Sachsen-Anhalt, Rheinland-Pfalz und Bremen sind besonders stark betroffen, hier sind mehr als die Hälfte der

Abgeordneten in den Datensätzen aufgetaucht. Auch sächsische Abgeordnete sind betroffen, jedoch in geringerem Umfang. Laut einer Recherche der Deutschen Presse-Agentur sind die offiziellen E-Mail-Adressen von etwa 8 Prozent der Abgeordneten in den gefundenen Datensätzen erschienen.

Die Risiken im Darknet

Frank Kromer, digitalpolitischer Sprecher der CDU-Fraktion, hebt die Wichtigkeit von Datensicherheit hervor und empfiehlt regelmäßiges Ändern von Passwörtern. Er betont, dass sichere Passwörter, die eine Mischung aus großen und kleinen Buchstaben, Zahlen und Sonderzeichen enthalten, dringend notwendig sind. Eamonn Maguire von Proton warnt jedoch, dass die im Darknet gefundenen Daten nur die „Spitze des Eisbergs“ darstellen.

Die Daten im Darknet sind oft das Ergebnis von Hackerangriffen und können für kriminelle Zwecke genutzt werden. Proton hat zusammen mit dem Cybersecurity-Unternehmen Constella Intelligence das Darknet nach diesen sensiblen Daten durchsucht. Ziel der Recherche ist es, ein umfassenderes Bild von der Sicherheitslage zu gewinnen, das auch Daten aus dem EU-Parlament und anderen europäischen nationalen Parlamenten umfasst.

Markt für gestohlene Zugangsdaten

Im Zusammenhang mit diesen Vorfällen wird eine besorgniserregende Marktbewegung im Darknet sichtbar. Cyberkriminelle handeln dort mit gestohlenen Zugangsdaten, oft für weniger als 1.000 US-Dollar. Laut einem Bericht von Check Point verkaufen Initial Access Broker, die für über 50% der Fälle verantwortlich sind, kompromittierte Unternehmenszugänge. Der Zugang zu Admin-Konten ist besonders gefragt, mit einem Anstieg von über 100% innerhalb eines Jahres.

Die große Nachfrage nach solchen Daten zeigt sich darin, dass

die Einstiegshürde für Cyberkriminelle durch die arbeitsteilige Struktur der Angriffe gesenkt wird. Die meisten illegal gehandelten Zugänge kosten between 500 und 3.000 US-Dollar, und besonders wertvolle Zugangsdaten werden nur selten für mehr als 10.000 US-Dollar angeboten. Diese Erschwinglichkeit könnte mehr Angreifer anziehen und die Sicherheitslage weiter verschärfen.

Cyber-Sicherheitslage in Deutschland

Die Cyber-Sicherheitslage in Deutschland hat sich in den letzten Jahren als zunehmend kritisch erwiesen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig Berichte, die wichtige Statistiken und Kennzahlen zur Cyber-Sicherheit in Deutschland und der Bundesverwaltung enthalten. Diese Berichte bieten Einblicke in die Herausforderungen und Bedrohungen im Bereich der Informationssicherheit und sind für Unternehmen sowie öffentliche Institutionen von großer Bedeutung.

Zahlreiche Unternehmen setzen oftmals nur auf grundlegende Sicherheitsmaßnahmen wie Windows Defender, was als unzureichend gilt. Um sich wirksam zu schützen, empfehlen Experten einen mehrschichtigen Sicherheitsansatz, einschließlich Multi-Faktor-Authentifizierung und kontinuierlicher Überwachung. Dies ist besonders wichtig, da gemäß BSI die meisten verkauften Zugangsdaten aus kleinen und mittleren Unternehmen stammen, die oft nicht ausreichend geschützt sind.

Der Vorfall und die darauf folgenden Warnungen verdeutlichen die dringende Notwendigkeit, die Cyber-Sicherheitsmaßnahmen zu verbessern, um das Vertrauen der Öffentlichkeit in die digitale Kommunikation und die Handlungsfähigkeit der Staatseinrichtungen nicht zu gefährden.

Details	
Vorfall	Cyberkriminalität
Ursache	Hackerangriffe
Ort	Sachsen-Anhalt, Deutschland
Quellen	• **www.freiepresse.de** • **www.it-daily.net** • **www.bsi.bund.de**