

Millionen Konten vor kriminellem Zugriff geschützt

Mit gestohlenen Zugangsdaten erbeuten Kriminelle jedes Jahr Milliarden Euro – den Schaden tragen Verbraucher und Anbieter gleichermaßen. Aus einem Forschungsprojekt zum Thema Identitätsdiebstahl gründet Dr. Matthias Wübbeling als Geschäftsführer die Identeco GmbH & Co. KG. Das Ziel ist klar: Verbraucher, Plattformanbieter und Unternehmen vor Betrug durch kriminelle Account-Übernahmen schützen.

Gestohlene Logindaten im Darknet

Die Bedrohung ist konkret: 80% der Cyberangriffe basieren auf gestohlenen Logindaten. Damit übernehmen Hacker nicht nur die Konten bei Onlineshops oder sozialen Netzwerken sondern sie dringen auch in Unternehmen ein. Gemeinsam mit seinen Kollegen sammelt Wübbeling im Darknet die gestohlenen Identitätsdaten. Alle Daten werden im ersten Arbeitsschritt anonymisiert. „So werden wir selbst nicht das Ziel von Hackern, denn bei uns gibt es ausschließlich verschlüsselte Daten in der Datenbank“, so Wübbeling. Diese Daten aber lassen sich von den Unternehmen nutzen, um gültige Zugangsdaten zu ermitteln. Neben Betrugsprävention lässt sich so auch SPAM-Aufkommen bei interaktiven Onlinediensten reduzieren. Betroffene Konten lassen sich einschränken, bevor Kriminelle diese übernehmen. Diese Maßnahmen sichern die eigene Infrastruktur und stützen das Vertrauen der Benutzer.

Aus Schaden wird man klug

„Oft muss das Kind erst in den Brunnen fallen“, sagt Wübbeling. Zugangsdaten müssen nicht beim eigenen Dienst abhandenkommen, vielmehr verwenden laut Identeco mehr als 50% der Benutzer dasselbe Passwort mehrfach für unterschiedliche Anbieter. Ist ein einzelner Account in den Händen Krimineller, ist das Risiko für alle anderen Onlinekonten dramatisch erhöht. Allerdings bekommt ein indirekt betroffener Anbieter vom erhöhten Risiko genauso wenig mit, wie der Benutzer. Einmal im Darknet zum Tausch angeboten, werden gestohlene Zugangsdaten fortan für Angriffe eingesetzt. Wübbeling und seine Kollegen schützen vor diesen Angriffen.

Nur echte Treffer!

Ein Kunde bei Identeco abonniert den Zugriff auf die kontinuierlich aktualisierte Leakdatenbank. Mit diesen Inhalten schützt man Mitarbeiter- und Kundenkonten: „Wir haben bereits mehrere Millionen Konten vor feindlicher Übernahme geschützt“, sagt Wübbeling stolz. „Bei uns sind alle Treffer auch echte Treffer“, da hilft nur die unmittelbare Sperre, oder zumindest die Einschränkung des Kontos. „Fehlalarme oder Unsicherheiten bei der Bewertung gibt es mit uns nicht“, sagt Wübbeling.

Innovative Ideen am Standort Bonn

Als ehemalige Bundeshauptstadt ist Bonn heute auch die Hauptstadt der IT-Sicherheit in Nordrhein-Westfalen – vielleicht sogar in ganz Deutschland. Das liegt an den Niederlassungen großer Unternehmen in Bonn, dem Bundesamt für Sicherheit in der Informationstechnik, Forschungseinrichtungen wie den ansässigen Fraunhofer-Instituten und der Ausrichtung der Universität mit ihrem Cyber Security Studiengang. Im Jahr 2020 wurde nach dem Forschungsprojekt „Effektive Information nach Digitalem Identitätsdiebstahl“ die Identeco GmbH & Co. KG gegründet. „Unsere Kunden sind etwa Plattformbetreiber wie New Work SE oder Payback, die Ihre eigenen Kunden schützen möchten.“ erläutert Wübbeling. Auch große und kleine Unternehmen aller Branchen können ihr Accountsicherheitsrisiko durch einen Lagebericht für ihre Mitarbeiterkonten einschätzen.

Kriminellen langfristig die Grundlage nehmen

Die kontinuierliche Sammlung von Leakdaten, datenschutzkonforme Aufbereitung und die prompte Bereitstellung zum Schutz der Benutzerkonten, das ist es, was die Identeco GmbH und Co. KG anbietet. „Insgesamt schützen wir heute bereits mehr als 100 Millionen Benutzerkonten bei unseren Kunden“, sagt Wübbeling und ergänzt: „In 5 Jahren möchten wir Marktführer der datenschutzkonformen Sicherheitsprodukte in Europa sein und weltweit Unternehmen vor Identitätsbetrug und Angriffen schützen“.

Ansprechpartner:

Identeco GmbH & Co. KG
Frank Zickenheimer
Mail: presse@identeco.de
Tel.: +49 (0) 228 286 285 81
www.identeco.de