E-Mail- und Passwortdiebstahl: Deutschland weltweit auf Platz 4 – „password, dragon, iloveyou, schalke04“ sind die am häufigsten im Dark Web gefundenen Passwörter

Cyberkriminalität gehört in Deutschland weiter zu den Bereichen mit dem höchsten Schadenspotenzial. Die durch den Branchenverband Bitkom e.V. errechneten Cybercrime-Schäden in Deutschland beliefen sich laut Wirtschaftsschutzbericht 2021 auf 223,5 Mrd. Euro jährlich und sind damit mehr als doppelt so hoch wie noch 2019.[1]

Laut Lagebericht Cybercrime des BKA[2] sind die zunehmende Digitalisierung und die Corona-Pandemie die Hauptgründe für den Anstieg der Kriminalität im digitalen Raum: Es gibt schlicht immer mehr Gelegenheiten für Taten. Immer neue Schnittstellen zwischen realer und digitaler Welt bilden zusätzliche Einfallstore für Hacker. Ob digitaler Impfnachweis, Online-Terminbuchungen oder -Geldtransfers – viele Dienstleistungen werden zunehmend auf digitalen Plattformen angeboten. Mit der Bedeutung des Internets für Privatpersonen, Unternehmen und staatliche Stellen nimmt auch die Anfälligkeit u.a. für Sabotage und Spionage zu. Im Zuge des Ukraine-Kriegs befürchtet das Bundeskriminalamt, dass es zu einer weiteren Zunahme an Straftaten im Netz kommen könnte.

Der aktuelle CRIF Cyber Report hat die Anfälligkeit von Einzelpersonen und Unternehmen für Cyberangriffe im Open und Dark Web untersucht und zeigt auf, welche Daten am meisten betroffen sind, welche Informationen im Web zu finden sind und wo sich der Datenverkehr konzentriert.

Für diese Studie hat CRIF im Vorjahr Websites, Gruppen, Foren und spezialisierte Gemeinschaften des sogenannten "Dark Web" durchsucht und Milliarden von Datensätzen analysiert. Dabei sind technologische Methoden zum Einsatz gekommen, die CRIF bereits für dessen eigene Cyber Risk Lösungen im Einsatz hat.

Deutschland auf Platz 4
Zu den Ländern, die aktuell am stärksten von E-Mail- und Passwortdiebstahl betroffen sind, gehören die USA, Russland, Frankreich und Deutschland, gefolgt von Großbritannien und Italien, das insgesamt auf Platz sechs liegt. Polen, Brasilien, Indien und Japan komplettieren die Top 10.

Des Weiteren wurde im Rahmen des Cyber Reports erhoben, welche Länder am stärksten von illegalem Kreditkartendatenaustausch betroffen sind. Dieses Ranking wird von den USA angeführt, gefolgt von Indien und Mexiko.

Online-Dating und Online-Spiele als Risiko
Konten, die mit Unterhaltungsseiten verknüpft sind, insbesondere Online-Spiele und Dating sind derzeit am stärksten dem Diebstahl persönlicher Daten ausgesetzt (48,6 Prozent aller Fälle). Ebenfalls stark betroffen sind Foren und Webseiten (22,9 Prozent), Streaming-Dienste (15,5 Prozent) sowie Social-Media Dienste (11,4 Prozent).

Diese Daten kursieren im Dark Web
Im Dark Web zirkulieren überwiegend persönlichen Daten, welche daher am anfälligsten sind. Es handelt sich um Passwörter, persönliche oder Firmen-E-Mail-Adressen, Benutzernamen und Telefonnummern. Diese wertvollen Kontaktdaten könnten für Betrugsversuche genutzt werden, etwa durch Phishing oder Smishing. Es werden aber auch finanziell relevante Daten ausgetauscht, wie z. B. Kreditkartendetails und IBANs.

Noch interessanter ist es, die Hauptkombinationen der abgefangenen Daten im Web zu beobachten. E-Mail-Adressen sind fast immer mit einem Passwort verbunden (94,7 Prozent der Fälle). Bei den im Dark Web gefundenen Passwörtern handelt es sich zumeist um persönliche E-Mail-Konten. Bei den Kreditkarteninformationen sind neben der Kartennummer beinahe immer auch die Kartenprüfnummer und das Ablaufdatum vorhanden (88,7 Prozent der Fälle). Zudem sind bei rund einem Fünftel der Fälle auch der Vor- und Nachname des Karteninhabers zu finden.

Die häufigsten Passwörter
Laut einer Analyse von Passwörtern, die im Dark Web gefunden wurden, waren die Top 10 der meistgenutzten Passwörter "123456", gefolgt von "123456789" und "qwerty". Dies sind sehr einfache Kombinationen aus Zahlen und

Buchstaben, die von Hackern leicht abgefangen werden können. In Deutschland befinden sich auf den ersten Plätzen: password, dragon, iloveyou, schalke04.

„Bei den Opfern handelt es sich typischerweise um Männer im Alter zwischen 41 und 50 Jahren. Es gibt zweifelsohne Verhaltensweisen, die die Risiken von Identitätsdiebstahl sinnvoll mindern können. Verbraucher sollten darauf achten, wie Passwörter, die mit verschiedenen Konten verbunden sind, festlegt und verwaltet werden. Passwörter sollten eben nicht "das übliche 1234" sein, sondern etwas komplexer und deshalb auch nicht so leicht zu durchschauen. Zudem sollte die Sensibilität erhöht werden, mit der Verbraucher auf E-Mails, Nachrichten oder Anrufe reagieren“, sagt CRIF Deutschland Geschäftsführer Dr. Frank Schlein.

Es ist auch wichtig, dass Benutzer, sofern möglich, die Zwei-Faktor-Authentifizierung aktivieren, um so zu verhindern, dass Hacker in Konten eindringen, selbst nachdem sie den Benutzernamen und das Passwort herausgefunden haben. Außerdem sollten Nutzer bei der Verwendung von öffentlichen WiFi-Netzwerken genau auf die Risiken achten, die mit der Speicherung von Anmeldedaten auf öffentlichen oder gemeinsam genutzten Computern verbunden sind.

Weitere Tipps und Tricks für den Umgang mit Risiken im Internet finden Sie auf unserem CRIF4ME-Blog:
https://www.blog.crif4me.de/

[1] https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf

[2] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html

Impressum

CRIF GmbH
Leopoldstraße 244
80807 München
Tel : 040 89803-0
Fax : 040 89803-777
E-Mail : **info.de@crif.com**
www.crif.de

Registergericht: AG München HRB 233802
Sitz der Gesellschaft: München
USt-IdNr.: DE117981371
Geschäftsführer: Dr. Frank Schlein, Carlo Gherardi, Marco Preti, Loretta Chiusoli

Registriertes Inkassounternehmen. Aufsichtsbehörde i.S.d. § 5 Abs. 1 Nr. 3 TMG: ist der Präsident des Amtsgerichtes München, Pacellistraße 5, 80333 München

Eingetragen im Rechtsdienstleistungsregister: 371 E - M 1809