Pressemeldung

Anstieg von Diebstahl von persönlichen Daten im Internet während der Corona-Pandemie. E-Mail- und Passwortdiebstahl: Deutschland auf Platz 4

Hamburg, 13. Juli 2021 – Im Zuge der Covid-19-Pandemie hat die Nutzung von digitaler Kommunikation in staatlichen Behörden, Forschungseinrichtungen und Unternehmen erheblich zugenommen – und dadurch die potenzielle Angriffsfläche von Cyber-Attacken deutlich erhöht und neuen Spielraum für Spionage, Ausspähung und Sabotage durch Cyberangriffe eröffnet.

Der Bundesverband der Deutschen Industrie e. V. (BDI) stellt aktuell fest, dass die deutsche Wirtschaft noch nie so stark angegriffen wie heute. Die Anzahl der Angriffe ist in der Corona-Pandemie weiter gestiegen, weil Unternehmen im Homeoffice noch verwundbarer sind[1].

Der aktuelle CRIFBÜRGEL 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.

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, die Tschechische Republik, Japan und Brasilien komplettieren die Top 10.

Des Weiteren wurde im Rahmen des Cyber Reports erhoben, welche Kontinente am stärksten von illegalem Kreditkartendatenaustausch betroffen sind. Dieses Ranking wird von Nordamerika angeführt, gefolgt von Europa und Asien, allerdings mit einem erheblichen Abstand zur Spitze. Am unteren Ende der Liste stehen Afrika und Ozeanien. Bei den einzelnen Ländern, die am stärksten betroffen sind, stehen die Vereinigten Staaten an der Spitze, gefolgt von Frankreich und Brasilien, die die Top drei vervollständigen.

Online-Streaming und Online-Spiele als Risiko

Konten, die mit Unterhaltungsseiten verknüpft sind, insbesondere Online-Spiele und Streaming, sind derzeit am stärksten dem Diebstahl persönlicher Daten ausgesetzt (51,5 Prozent aller Fälle). Ebenfalls stark betroffen sind soziale Netzwerke (31,8

[1] https://bdi.eu/#/artikel/news/angriffe-auf-deutsche-wirtschaft-nehmen-zu/

Prozent), gefolgt von E-Commerce (10,7 Prozent) sowie Foren und Webseiten (5,9 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 (96,3 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 (98,6 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.

„Bei den Opfern handelt es sich typischerweise um Männer im Alter zwischen 41 und 60 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. Zudem sollte die Sensibilität erhöht werden, mit der Verbraucher auf E-Mails, Nachrichten oder Anrufe reagieren“, sagt CRIFBÜRGEL 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.

Über die Studie

Für diese Studie hat CRIF im 2. Halbjahr 2020 Websites, Gruppen, Foren und spezialisierte Gemeinschaften des sogenannten "Dark Web" durchsucht und Milliarden von Datensätzen analysiert. Dabei sind technologische Methoden zum Einsatz gekommen, welche CRIF bereits für dessen Cyber Risk Lösungen im Einsatz hat.

Über CRIFBÜRGEL

Die CRIF Bürgel GmbH ist in Deutschland einer der führenden Informationsdienstleister für Firmen und Privatpersonen und kann auf über 130 Jahre Markterfahrung verweisen. Das Unternehmen bietet passgenaue Lösungen für die Identifikation, Bonitätsprüfung und Betrugsprävention, für Kreditrisiko- und Adressmanagement sowie zu Digitalisierung und Predictive Analytics für Unternehmen und Finanzinstitute. CRIFBÜRGEL gehört zur global agierenden Wirtschaftsauskunftei-Gruppe CRIF mit Hauptsitz in Bologna, Italien. Weitere Informationen unter: www.crifbuergel.de

Pressekontakt: Kerstin Valet, k.valet@crifbuergel.de