UIMCommunic@tion
praxisnah.gut.informiert.

02/2024
Ausgabe für Deutschland

„Mother of all Breaches“ zwingt zum Nachdenken über Passwörter

Authentifizierungsmethoden sollten auf den Prüfstand

Aktuell überschlagen sich die News zur „Mother of all Breaches“ (MOAB). Was steckt dahinter? IT-Sicherheitsexperten sprechen vom größten Datenleck, das bisher entdeckt wurde. Andere Spezialisten wiederum vermuten eine Werbeaktion hinter der Nachricht von sage und schreibe 26 Milliarden Datensätzen, die im Netz aufgetaucht sein sollen. „Ob es sich um einen Werbegag oder die Realität handelt, ist weniger entscheidend. Es zeigt die Relevanz der eigenen Informationssicherheits-Organisation“ erklärt UIMC-Geschäftsführer Dr. Jörn Voßbein zur aktuellen Berichterstattung. Für ihn und das UIMC-Team rückt dabei das Thema Passwort und insbesondere die Passwortqualität in den Mittelpunkt. Um was für Datensätze es sich handeln soll, welche Passwörter besonders beliebt sind und wie sich die eigene Sicherheit steigern lässt, dazu mehr im Folgenden.

Was für Datensätze umfasst die „Mother of all Breaches“? Die Daten stammen angeblich von mehreren bekannten Online-Diensten, darunter Twitter (X), Telegram, Dropbox, Deezer, LinkedIn, Adobe, Canva und Badoo. Allein zwei Milliarden Einträge werden den chinesischen Unternehmen Tencent und Weibo zugeschrieben. Aber auch von den anderen genannten Diensten sollen jeweils mehrere Millionen Datensätze enthalten sein. Darüber hinaus seien in MOAB auch Daten mehrerer Regierungsbehörden vertreten, darunter solche aus den USA, Brasilien und Deutschland. Allerdings wird bereits vom zuerst berichtenden Dienst Cybernews eingeräumt, dass es sich um ein Gesamtpaket von Datensätzen handelt, die aus früheren Datenleaks bekannt sind. Es bleibt abzuwarten, ob es sich tatsächlich um die MOAB handelt oder „nur“ um einen geschickten Marketing-Zug zum „Ändere-Dein-Passwort-Tag“.

Apropos Passwort: Die beliebtesten Passwörter in 2023 wurden wieder anhand von geleakten Daten festgestellt. Nachfolgend die zehn beliebtesten: 123456789, 12345678, hallo, 1234567890, 1234567, password, password1 und target123.

Tipps: Klar ist, dass solche Passwörter die Arbeit von Cyberkriminellen sehr erleichtern. Deshalb appellieren UIMC und viele andere IT-Sicherheitsexperten eindringlich an alle Nutzer, ein starkes Passwort bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zu kreieren und dieses dann auch regelmäßig zu erneuern. Außerdem sollte niemals bei zwei Plattformen mit dem gleichen Passwort agiert werden, da ansonsten nach dem ersten Hack eine Domino-Effekt entstehen kann. „Durch diese simplen und kostenarmen Maßnahmen lässt sich die eigene Datensicherheit erheblich steigern. Wenn Hacker zu lange brauchen, um das Passwort zu knacken, verlieren sie schnell die Lust“, erläutert Dr. Jörn Voßbein. Um möglichst komplexe Passworte zu nutzen, können auch sog. „Passwort-Safes“ ge-

WICHTIGE INFO: Aufsichtsbehörde führt Überprüfungen durch

Das BayLDA führt flächendeckende Prüfungen zu verschiedenen Schwerpunktthemen durch; andere Aufsichtsbehörden agieren ähnlich. Aktuell wird überprüft, ob im Verzeichnis von Verarbeitungstätigkeiten (VvV) auch eine Risikobewertung durchgeführt wurde und ob diese eine Datenschutzfolgenabschätzung erforderlich macht. Jedes Unternehmen sollte daher überprüfen, ob ihr VvV vollständig ist; sinnvollerweise gemeinsam mit dem Datenschutzbeauftragten. **Übrigens:** Der UIMC-Master erfüllt die Anforderungen.

Zu finden im www.online-formular-center.eu (zugangsbeschränkt)

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

nutzt werden, die bei einer guten Implementierung das Niveau steigern können. Auch sollte dann, wenn eine Zwei-Faktor-Authentifizierung angeboten wird, diese auch genutzt werden. Dies sollte auch in Unternehmen stärker diskutiert werden, bei dem neben dem Passwort (Wissen) durch einen zweiten Faktor (Besitz; als ein z. B. Code per SMS, App oder Token) die Schwierigkeit für Hacker erhöht, in ein Konto einzudringen.

Fazit

Ganz gleich ob MOAB nun neue Daten liefert oder nur aus früheren Datenlecks zusammengewürfelt wurde, sollten User die existierenden Gefahren nicht unterschätzen. Gleichzeitig gilt es, starke Passwörter zu setzen und diese regelmäßig einem Update zu unterziehen. Denn auch wenn die Daten schon älter sind, lassen sie sich möglicherweise noch immer effektiv für Phishing-Kampagnen und andere Social Engineering-basierte Angriffe ausnutzen.

IT-Trends digital und sicher, **20.03.2024, Bochum**

Mit Gutschein-Code kostenfrei!

ZD4-4T2-SCA-QZ5 (First Order, first serve)

UNSER VORTRAG AUF DER IT-TRENDS „DIGITAL UND SICHER“

Love, Peace & Compliance: Mit dem etwas anderen Ansatz Datenschutz und Informationssicherheit im Mittelstand pragmatisch umsetzen

In vielen Unternehmen wird zwar an Compliance im Sinne von Datenschutz und Informationssicherheit gedacht, doch oftmals nicht wirklich umgesetzt. Dies hat unterschiedliche Gründe, die aber immer wieder im „Faktor Mensch“ münden. Hierbei sind aber nicht nur der User, sondern auch die Fachbereiche und die Geschäftsleitung zu betrachten.

Innerhalb des Vortrags zeigen wir, worin die Probleme konkret liegen, auf welche Faktoren bei Projekten zur Umsetzung von Datenschutz und Informationssicherheit zu achten sind und mit welchen Tricks eine Verbesserung erreicht werden kann… auch ohne teure Tools und Berater.

Der Fachbesucher erhält nicht nur einen Überblick über typische Problemstellungen in der Umsetzung von Compliance, sondern auch pragmatische Lösungsansätze. Eigene Fragestellungen können gerne diskutiert werden.

Unser Referent: Tim Hoffmann

Aktuelles im Online-Formular-Center

Um über Neuerungen zeitnah informiert zu werden, können Sie unser News-Forum abonnieren und erhalten daraufhin eine E-Mail, sofern Sie einen personalisierten Account haben.

www.uimcollege.de