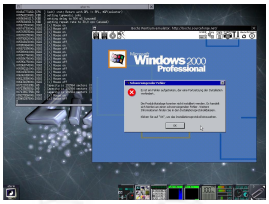

Großteil ändert Passwort nach Datenleck nicht - Zwei von drei Usern ignorieren Sicherheitslücken oft - Neue Zugangs-Codes selten sicher

Zwei von drei Menschen ändern ihr Passwort nach einem Datenleck nicht. Wenn eine Domain öffentlich bekannt gibt, dass ihre Cybersecurity durchbrochen wurde, greifen die meisten Nutzer dieser Domain nicht zu Sicherheitsmaßnahmen, wie eine Studie der Carnegie Mellon University ergibt.

Nutzer bleiben Monate inaktiv

"Besonders besorgniserregend ist, dass die neuen Passwörter oft sehr ähnlich wie die anderen Zugangscodes von Anwendern sind. Außerdem ändern Menschen auch selten ihre Passwörter in anderen Domains, auch wenn diese identisch mit denen auf den Seiten sind, die von Datenlecks betroffen sind", schreiben die Studienautoren.

Für die Studie haben die Forscher Informationen von den Heim-Computern von 249 Menschen gesammelt. Von den Studienteilnehmern hatten 63 einen Account bei einer Domain, die zwischen den Jahren 2017 und 2018 ein Datenleck meldeten. Nur 21 davon änderten auf der Seite ihr Passwort. Sechs von diesen Studienteilnehmern haben mehr als drei Monate gebraucht, um aktiv zu werden.

Neues Passwort oft schwächer

Lediglich ein Drittel der User, die Passwörter geändert haben, suchten sich stattdessen einen stärkeren Sicherheitscode aus. Der Großteil wechselte auf einen weniger sicheren Code. Dem Team zufolge ist vielen Menschen nicht klar, was ein starkes Passwort ausmacht. Sie empfehlen deswegen die Verwendung eines Passwort-Managers, der automatisch starke Passwörter erstellt. Jedoch hat eine Studie der University of York von März 2020 auch Passwort-Manager als mögliche Sicherheitslücke identifiziert.