Ebersbacher Zeitung

Mittwoch, 6. Mai 2020

Handel mit Passwörtern für Zoom

Der Verdacht, dass jemand Zugriff auf die eigenen Internetkonten und Internetdienste haben könnte, lässt niemanden ruhig schlafen. Und der Verdacht ist nicht unbegründet: Aktuell werden im Dark Web hunderttausende Datensätze mit Log-in-Informationen für den Videochat-Dienst Zoom zum Kauf angeboten, berichtet das IT-Fachportal „Bleepingcomputer.com".

Wahrscheinlich handle es sich dabei um Log-In-Informationen bereits länger zurückliegender Hackerangriffe oder Datenlecks bei Diensten, bei denen Nutzerinnen und Nutzer die gleichen Benutzernamen und Passwörter benutzen wie aktuell bei Zoom. Der Zusammenhang: Hacker, die Anmelde-Informationen für einen Dienst erbeuten, probieren diese meist bei vielen anderen populären Seiten aus. Denn sie können sich darauf verlassen, dass viele Nutzer ihre Passwörter mehrfach benutzen.

Internetnutzer sollten daher jetzt und grundsätzlich kontinuierlich prüfen, ob auch Log-in-Daten von ihnen ins Netz gelangt und dort mehr oder weniger frei auffindbar sind, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI). Helfen können dabei Datenbanken, in die Sicherheitsforscher nach Hackerangriffen oder Datenlecks kompromittierte Zugangsdaten einpflegen – etwa die Pwned"-Abfrage des IT-Sicherheitsforschers Troy Hunt. Mozillas Abfragedienst Firefox Monitor greift auf die Datenbank von „Have I been pwned?" zurück, arbeitet nahezu identisch, unterscheidet sich aber durch ein praktisches Detail: Weil das Ergebnis der Abfrage nur für den Moment gültig ist, kann man sich auf der Monitor-Seite auch mit einer Mail-Adresse registrieren und bekommt dann sofort Bescheid, falls eigene Daten im Netz auftauchen sollten.

Mit dem Identity Leak Checker bietet das Potsdamer Hasso-Plattner-Institut (HPI) eine weitere Abfragemöglichkeit an. Auch hier müssen E-Mail-Adressen angegeben werden. Per Datenbank-Abgleich wird dann geprüft, ob die Mail-Adresse in Verbindung mit anderen persönlichen Daten wie Telefonnummer, Geburtsdatum oder Adresse im Internet offengelegt wurde und missbraucht werden könnte. Gibt es bei einem der Dienste einen Treffer, sollte das Passwort geändert und nicht weiter verwendet werden. Achtung: Wenn ein Passwort in keiner der Datenbanken steht, bedeutet nicht, dass es sicher ist. Onlinekonten sollten nicht nur mit starken, sondern mit individuellen Passwörtern und möglichst einer Zwei-Faktor-Authentifizierung geschützt werden. *dpa*