Ende einer Legende

Nachdem sich die amerikanische Standardisierungsbehörde NIST schon vor zwei Jahren vom guten alten Passwortwechsel verabschiedet hat, den bis dato (nicht nur) Admins regelmäßig gefordert hatten, zieht nun das BSI endlich nach: Das gerade in neuer Ausgabe erschienene BSI-Grundschutz-Kompendium enthält unter „ORP.4.A8 Regelung des Passwortgebrauchs“ keine Forderung mehr nach regelmäßigem Wechsel des Passworts.

Hieß es noch in einer früheren Grundschutzversion unter „M 2.11 Regelung des Passwortgebrauchs“: „Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage“, so schwächte die 2019er-Ausgabe den Passus bereits ab zu: „Die Passwörter SOLLTEN in angemessenen Zeitabständen geändert werden.“ Nun ist die Forderung endgültig abgeschafft – was viele Experten begrüßen, denn die Sinnhaftigkeit einer Regel, die von Nutzern durch minimale Änderungen ausgehebelt werden kann (à la Passwort1, Passwort2, Passwort3 …), bezweifelten viele.

Was nur wenige wissen: Im Grunde war die Regel seinerzeit ohnehin nur durch die ungeschickte Auslegung eines Hinweises des NIST entstanden. Dieses hatte im Jahr 2004 im Appendix A der Special Publication 800-63 die Abhängigkeit zwischen der Entropie von Passwörtern und deren Gültigkeit untersucht. Im Ergebnis besagte der Standard sinngemäß, dass eine geringere Entropie durch Passwortwechsel kompensiert werden könne. Dazu müsse die Gültigkeit eines Passwortes kürzer gewählt sein als der für das Brechen des Passwortes per Brute-Force-Angriff benötigte zeitliche Aufwand.

Dieser – im Standard allgemein gehaltene – Hinweis führte zu der Interpretation, dass Passwörter in regelmäßigen Intervallen zu ändern seien, um als sicher zu gelten. In letzter absurder Konsequenz hieße das: Wenn beispielsweise – wie bei LinkedIn schon mehrfach geschehen – die Passwort-Hashes durch eine Sicherheitslücke oder schlechte Konfiguration den Falschen in die Hände fallen und die Passwörter mit vorgefertigten Rainbow-Tables binnen weniger Stunden offengelegt sind, wäre man nur mit einem täglichen Passwortwechsel safe.

Was also tun? Auf jeden Fall ein laaaaaaanges, sicheres Passwort wählen. Denn entgegen landläufiger Meinung ist ein solches in der Regel auch noch nach Jahren sicher. Und: Wo immer es möglich ist, einen zweiten Faktor einsetzen.

UTE ROOS