6 EINFACHE REGELN FÜR IHRE PASSWORT-RICHTLINIE

Oder auch: Machen Sie Ihr Unternehmen ganz einfach sicherer

01.

RICHTLINIEN MÜSSEN EINFACH SEIN

Notieren Sie die wichtigsten Punkte knapp und übersichtlich, z.B. geforderte Passwortlänge, -komplexität und höchstmögliche Anzahl erfolgloser Anmeldeversuche.

02.

DIE RICHTLINIEN GELTEN FÜR ALLE (AUCH DEN CHEF)

Die Passwort-Richtlinien gelten für alle Mitarbeiter, egal auf welcher Ebene, also auch Inhaber, Vorstand und Management. Ausnahmen gibt es nicht.

03.

LEGEN SIE EINE „SCHWARZE LISTE“ AN

Darin sollten häufig verwendete schlechte Passwörter dokumentiert werden („admin“ oder „12345“ zum Beispiel). Sorgen Sie dafür, dass diese gar nicht erst gewählt werden können.

04.

SPEICHERN SIE MITARBEITER-PASSWÖRTER SICHER

Speichern Sie sie als Salted Hashes und arbeiten Sie mit einem Hashing-Algorithmus, der speziell für die Speicherung von Passwörtern entwickelt wurde.

05.

STÄNDIG NEUE PASSWÖRTER? NICHT NÖTIG

Sowohl das NIST (National Institute for Standards and Technology) als auch das britische NCSC (National Cyber Security Centre) empfehlen, Passwörter nur dann zu ändern, wenn der Nutzer dies wünscht oder wenn Hinweise vorliegen, dass das Passwort kompromittiert worden ist. Werden Nutzer zur regelmäßigen Änderungen ihrer Passwörter gezwungen, neigen sie dazu, einfache und leicht zu merkende Passwörter zu wählen oder ihre bestehenden Passwörter nur minimal und immer wieder gleich zu ändern (z.B. durch Hinzufügen eines Buchstaben oder einer Zahl am Ende des bisherigen Passworts).

06.

AUCH IOT-GERÄTE GEHÖREN DAZU!

Ihre Passwort-Richtlinie muss unbedingt alle im Unternehmen verwendeten Geräte und Systeme erfassen. Vor allem IoT-Geräte wie Kameras, Smart Hubs oder Router werden häufig vergessen und sind dadurch beliebtes Einfallstor für Angriffe.