Optionale Standortsicherheits-einstellungen in den Portaleigenschaften

Relias Learning GmbH Tel.: 0800 72 34 784 E-Mail: kundenbetreuung@relias.de
D-09/2023

Optionale Standortsicherheitseinstellungen

Das Relias LMS verfügt über optionale Sicherheitseinstellungen (siehe Abbildung 1). Im Laufe Ihres Onboarding-prozesses werden diese Einstellungen mit Ihnen besprochen. Sie können diese aber mit Unterstützung der Kundenbetreuung im Nachgang anpassen lassen.

Folgende Funktionen stehen Ihnen zur Verfügung:

- Inaktivität Timeout (in Minuten)
- Passwortablauf (in Tagen)
- Passwort Lockout (in Versuchen)
- Passwort-Reset bei erster Anmeldung
- Erfordert komplexes Passwort
- Einschalten der Einschränkungen der Passwortgeschichte

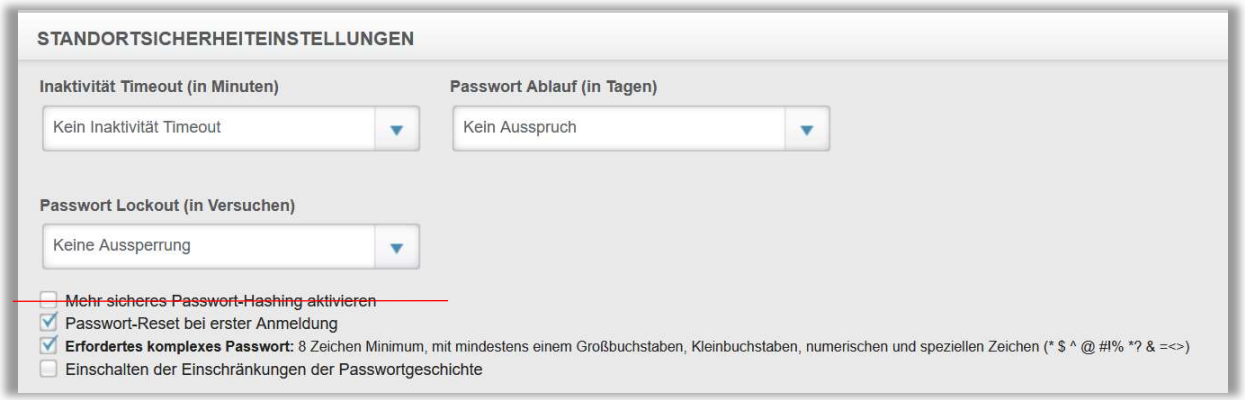

Abbildung 1 - optionale Sicherheitseinstellungen

Bitte beachten Sie:

Die Option „Mehr sicheres Passwort-Hashing aktivieren“ ist Teil der Funktion „Analytics and Assessments“, die in Deutschland noch nicht in Verwendung ist.

Sie erhalten nachfolgend eine Beschreibung der einzelnen Sicherheitseinstellungen.

Inaktivität Timeout

- Mit dieser Sicherheitseinstellung kann bestimmt werden, dass Lernende nach einer Inaktivität im Relias LMS automatisch nach 15, 30, 45 oder 60 Minuten abgemeldet werden
- Wenn ein*e Nutzer*in automatisch abgemeldet wird, erhält er*sie eine Mitteilung, dass aufgrund von Inaktivität die Abmeldung vorgenommen wurde und eine Aufforderung, sich erneut anzumelden

Passwortablauf

- Mit dieser Option besteht die Möglichkeit, Passwörter nach 30, 60 oder 90 Tagen ablaufen zu lassen
- Der*Die Nutzer*in wird 30 Tage vor Ablauf des Passworts und anschließend täglich per E-Mail über den Ablauf des Passwortes informiert
- Zu jedem Zeitpunkt dieser 30 Tage haben die Nutzer*innen die Möglichkeit, das Passwort zu ändern, bevor sie am letzten Tag dazu aufgefordert werden

Passwort Lockout

- Mit Aktivierung dieser Sicherheitseinstellung besteht die Möglichkeit, Nutzerkonten zu sperren, wenn aufeinanderfolgende erfolglose Anmeldeversuche stattgefunden haben, zum Beispiel, weil das Passwort zu oft falsch eingegeben worden ist
- Nutzerkonten können somit nach 2, 3, 6, 12 oder 20 erfolglosen Versuchen gesperrt werden
- Ist der Zugang zum Nutzerkonto gesperrt, erhält der*die Nutzer*in eine Mitteilung, die darüber informiert, dass das Konto gesperrt wurde
- Wenn ein*e Nutzer*in zu einer Einrichtung gehört, welche es ermöglicht, dass Passwort selbstständig zurückzusetzen, kann er*sie dies tun oder sich an Administrierende wenden, um das Konto freizuschalten zu lassen
- Für eine Einrichtung, die es Nutzer*innen NICHT erlaubt, das Passwort selbstständig zurückzusetzen, muss er*sie sich an Administrierende wenden, um das Konto freizuschalten zu lassen
- Administrierende können das Nutzerkonto auf der Profilseite freischalten

Passwort-Reset bei erster Anmeldung

- Mit Aktivierung dieser Option werden Nutzer*innen nach erstmaliger Anmeldung aufgefordert, das Passwort zu ändern

Erfordertes komplexes Passwort

- Wenn diese Sicherheitseinstellung aktiviert ist, müssen Passwörter mindestens 8 Zeichen, einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein nicht-alphanumerisches Zeichen enthalten

Einschalten der Einschränkung der Passwortgeschichte

- Diese Sicherheitseinstellung gibt vor, wie oft ein in der Vergangenheit verwendetes Passwort erneut verwendet werden darf
- Zusätzlich verhindert diese Einstellung, dass Nutzer*innen ihre vier neusten Passwörter beim Ändern seines*ihres Passwortes wiederverwenden können
- Diese und die Sicherheitseinstellung für den Ablauf des Passwortes sind nicht voneinander abhängig, jedoch ergänzen diese sich, um die Passwörter zu schützen