Trustelem password levels

Trustelem password levels

Trustelem passwords have 3 security levels : **None** - **Medium** - **High**

Trustelem uses a security framework, **zxcvbn** (https://github.com/dropbox/zxcvbn) developed by Dropbox, which evaluates password strength according to current best practices and dictionaries.

Basically, zxcvbn looks for **patterns** in the password, and searches for these patterns in current pattern/password dictionaries. We also add our own dictionary, which contains account information (login, domain, orga...). Based on this, it will define a security score.

Our **Medium** level = zxcvbn score of 3 (safely unguessable: moderate protection from offline slow-hash scenario.)
Our **High** level = zxcvbn score of 4 (very unguessable: strong protection from offline slow-hash scenario)

To this framework, we add the length defined on Trustelem.

Why is it secure ?

There are no explicit criteria such as "X capitals, Y special characters...", but rather a live calculation of password strength based on a constantly updated dictionary. This is much more secure.

Password creation requirements are generally the same on most websites. Hackers therefore know what patterns to look for, such as replacing letters with symbols (@ for a, for example). Traditional password security requirements would accept "P@ssw0rdSecure" as a password, even if it is not secure at all.

On Trustelem, administrators can easily enforce password requirements, as the feature enables employees to create secure passwords with ease. Companies can therefore ensure that their employees adopt better password habits, without disrupting their working day or the company.

Revision #1
Created 18 April 2024 08:17:47 by WALLIX Admin
Updated 18 April 2024 08:47:47 by WALLIX Admin