Requisitos para una contraseña robusta

Las contaseñas son métodos de protección de datos que preservan la confidencialidad de todo tipo de información.

Por lo tanto, vulnerar las contraseñas de un usuario es una acción de alto valor para un atacante, por lo que desde wizardsoft Argentina recomendamos usar contraseñas fuertes y robustas.

Es interesante que diferencies lo que es una contraseña debil y una contraseña fuerte.

Contraseña débil

Una contraseña débil sería una que fuese muy corta, que fuese una predeterminada, o una que pudiera adivinarse rápidamente al utilizar una serie de palabras que son posibles encontrar en diccionarios. (ej:nombres propios o palabras basadas en variaciones del nombre del usuario).

Como ejemplos de contraseñas débiles podemos mencionar las siguientes: administrador, 1234, nombre del usuario, xx/xx/xx – fechas importantes, ya que la mayoría de estas se encuentran en bases de datos o en diccionarios de búsqueda para ataques (dictionary search attack).

Contraseñas Fuertes

A la hora de elegir una contraseña te recomendamos:

- Que esté formada por 8 caracteres o más
- Que sea una combinación de los siguientes 3 tipos de caracteres:

- Letras en minúsculas (de la a a la z)

- Letras en mayúsculas (de la A a la Z)

Requisitos para una contraseña robusta
- Números (del 0 al 9)

- Además, si quieres darle mayor seguridad puedes utilizar:

- Caracteres especiales (çÇ@áéíóúäëïöüàèìòùñ.[ ] _-¡!#*/)

La utilización de contraseñas fuertes acarrea para el usuario una dificultad básica, ya que suelen ser más complejas de recordar que las simples. Para mitigar este inconveniente, existen dos alternativas:

- Utilizar contraseñas fuertes, pero recordables a través de reglas

nemotécnicas.

- Utilizar alguna aplicación para almacenarlas de forma cifrada y segura

http:/es.wikipedia.org/wiki/Gestor_de_contraseñas

Como se puede observar, la utilización de contraseñas fuertes no es una tarea compleja para el usuario y de ésta forma, con medidas sencillas y básicas, puede prevenir gran cantidad de problemas y minimizar considerablemente la posibilidad del robo de información.

Para que una contraseña sea considerada “fuerte”, la misma debe ser lo suficientemente larga y generada al azar. En el mejor de los casos, debería ser creada únicamente por la persona que la utilizará.

Algunos ejemplos de contraseñas fuertes: taSty@wheeT34, Partei@34! y #23kL!Lflux. Como podemos ver, se utilizan combinaciones de letras mayúsculas, minúsculas, de números y de símbolos.