OPINIÓN / DESPUÉS DE LA PANDEMIA

Las malditas contraseñas

por Enrique Dans · 25 mayo, 2022 - 01:50 GUARDAR

Un estudio muy reciente sobre el uso de contraseñas y la ciberseguridad ha encontrado lo miso que muchos estudios anteriores: que las contraseñas más habituales son cosas como "012345678", "password" o "qwerty123". La diferencia entre este estudio y otros anteriores no está en sus conclusiones, sino en su público objetivo: en esta ocasión, los autores del estudio limitaron la muestra, en lugar de a usuarios en general, a directivos de compañías.

¿Qué lleva a un directivo de una compañía, al que se supone un mínimo de formación y de responsabilidad, a utilizar una **contraseña tan profundamente estúpida** que no solo es que pueda ser averiguada en cuestión de segundos con cualquier herramienta de las utilizadas habitualmente por un delincuente, sino que incluso está entre las primeras que probaría cualquier aficionado? ¿Cómo se puede ser tan profundamente irresponsable?

La cuestión tiene una especial importancia cuando sabemos que la frecuencia de ciberataques a compañías ha crecido de manera brutal en los últimos tiempos, y que se ha incrementado además su nivel de gravedad. Hoy, recibir un ciberataque de *ransomware* que paralice la actividad de tu compañía y exija un pago de un rescate no solo no resulta excepcional, sino que es ya casi norma.

Los delincuentes se dedican, simplemente, a recorrer listados de compañías de todos los tamaños buscando víctimas, y simplemente adaptan la petición de rescate a su facturación.

Con tener un nombre de usuario -que puede deducirse fácilmente del nombre de un directivo- y adivinar una contraseña, ya estás dentro y puedes hacer lo que quieras.

> *Sigue habiendo idiotas que tienen como contraseña 12345678 o password o qwerty123*

Además, se usan muchos otros tipos de herramientas en algunos casos muy sofisticadas, pero podría ser así de fácil. Y sin embargo, sigue habiendo idiotas que tienen como contraseña "12345678" o "password" o "qwerty123", y que simplemente merecerían que sus compañías los pusieran de patitas en la calle y alegasen además que se trata de un despido perfectamente justificado. Lo mismo que harías con un empleado que reiteradamente dejase por la noche **la puerta de la calle abierta y la alarma sin conectar.**

Para las aseguradoras, la cuestión está adquiriendo una dimensión cada vez más importante: sus clientes reclaman cada vez más protección, pero sus prácticas son en general un desastre, y la cultura de ciberseguridad brilla por su ausencia.

Las **aseguradoras**, en estos casos, están elevando sus tarifas para intentar cubrirse frente a daños mucho más frecuentes y más cuantiosos. Pero obviamente, esa no es la solución.

En breve, empezaremos a ver aseguradoras que simplemente se niegan a asegurar a compañías que no hayan pasado una prueba de intrusión externa, hecha por compañías como HackerOne y similares, que emplean a *hackers* de todo el mundo para tratar de encontrar vulnerabilidades en sus clientes.

La gran mayoría de las compañías, de hecho, aún **están en la prehistoria de la seguridad**, y siguen pidiendo a sus empleados que cambien su contraseña cada poco tiempo, que escojan una que contenga todo tipo de caracteres extraños, y que no se parezca a ninguna de las anteriores.

¿Son esas empresas conscientes de la estupidez que están pidiendo a sus empleados? Si a una persona le dices que su contraseña va a ser ya de por sí difícil de recordar, y que además se la vas a cambiar cada poco tiempo, ¿qué esperas que haga?

En el mejor de los casos, que busque reglas mnemotécnicas básicas para recordarla. Y en el peor, apuntarla en una nota adhesiva y pegarla en la pantalla... o simplemente, poner la contraseña más fácil de recordar que se le ocurra.

La realidad es que **cualquier contraseña que podamos recordar es una mala contraseña**, y que lo que deberíamos hacer es utilizar un gestor de contraseñas, idealmente, con licencia corporativa.

De esa manera, la responsabilidad de mantener y cambiar las contraseñas pasa de los empleados a la empresa, y se puede llevar a cabo de manera mucho más profesionalizada (y esa necesidad existe, porque periódicamente, alguna contraseña aparece en algún volcado de información y hay servicios que nos avisan de ello).

Con un gestor de contraseñas, el único problema es dar la orden de cambiarla, y que el empleado utilice su aplicación, en el navegador o en el *smartphone*, para introducirla. Hoy, una contraseña no solo no debe recordarse... ies que ni siquiera debemos teclearla!

En la práctica, las compañías que de verdad saben de qué hablan llevan ya algún tiempo hablando de **jubilar las contraseñas y sustituirlas por una combinación de elementos biométricos** y de autorización de doble clave. Tras la autenticación en un dispositivo o entorno nuevo, recibes una clave en una app de autenticación en tu smartphone, y debes introducirla también.

El uso de una app de autenticación de doble factor es tan sencillo y tan poco molesto, que deberíamos utilizarlas en todos los servicios mínimamente críticos.

En estos momentos, y con la que está cayendo con grupos de ciberdelincuentes dedicados a buscar víctimas, desarrollar una cultura de ciberseguridad es más importante que nunca.

Y en muchos casos, y para muchas compañías, una cultura de ciberseguridad es precisamente lo contrario de lo que llevan mucho tiempo haciendo: martirizando a sus empleados con peticiones estúpidas que no sirven para nada, o que incluso empeoran la seguridad. Es el momento de **replantearse esas prácticas**, y sobre todo, de hacer mucha pedagogía sobre la importancia del tema, que alcance a toda la organización: desde el CEO, hasta el último empleado.

SIGUE LOS TEMAS QUE TE INTERESAN
CIBERSEGURIDAD COLUMNAS DE OPINIÓN

1

MÁS DE ENRIQUE DANS

- Ciberseguridad: el nivel de las amenazas crece
  18 mayo, 2022 - 03:21
- El mercado y el péndulo
  11 mayo, 2022 - 03:22
- La medicina como ciencia de datos
  4 mayo, 2022 - 03:55
- ¿Qué va a hacer Musk con Twitter?
  27 abril, 2022 - 03:45

LOS ÚLTIMOS

HABLANDO EN DIGITAL
Liderazgo en la era digital
Francisco Hortigüela


INCERTIDUMBRES Y UTOPÍAS
Startups, ¿se acabó la fiesta?
Francisco Estevan


ALFABETIZACIÓN DIGITAL E INNOVACIÓN
Por qué en Silicon Valley alejan a los niños de las pantallas
Laura Cuesta Cano


La prueba de fuego de las criptomonedas
Juan Ignacio Crespo


Ahora en portada

DESPUÉS DE LA PANDEMIA
Las malditas contraseñas
Enrique Dans


LA TRIBUNA
El sobreesfuerzo de pagar el alquiler en España
María Martos

1 Comentario

Escribe tu comentario

NORMAS DE USO
ENVIAR

Por fecha Por relevancia