Blog ECIJA 2.0

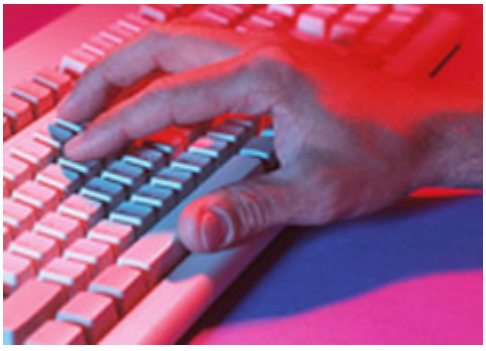
25 de Octubre de 2018

Javier Arnaiz

abogado de ECIJA

Un enemigo para la ciberseguridad: el usuario

"Por favor, utilice una contraseña única que sea difícil de identificar y que no contenga caracteres que puedan asociarse fácilmente con su persona". En numerosas ocasiones, este mensaje puede ser el inicio de un acceso masivo a todas las cuentas del usuario por usar la misma contraseña insegura en el correo, las redes sociales y la app de pagos: Jose1990 (el nombre y el año de nacimiento).



Los expertos en ciberseguridad lo vienen anunciado desde hace tiempo, el principal riesgo y la mayor amenaza para la seguridad de los usuarios no son los ciberterroristas ni las grandes vulnerabilidades de los sistemas, sino el propio usuario del equipo o de las aplicaciones.

Para tener una idea del alcance de este riesgo, se puede analizar la

con este estudio, es que desde 2014 la contraseña más utilizada es "123456", pero es que si se analizan el resto de contraseñas de esta clasificación se puede ver cómo acceder a muchos sistemas o dispositivos es tan sencillo como probar combinaciones muy sencillas como "password" o "iloveyou".

El riesgo del uso de estas contraseñas tan inseguras además tiene otro aspecto importante, y es que en numerosas ocasiones el usuario repite las mismas en las diferentes aplicaciones y plataformas, permitiendo un potencial acceso masivo muy sencillo a una cantidad ingente de información.

Otro de los riesgos que se puede encontrar vinculado a las contraseñas es el almacenamiento de las mismas en lugares no seguros o no preparados para ello. Como ejemplo, Ian Balina (un reconocido *youtuber* experto en criptomonedas) supuestamente sufrió un acceso a sus cuentas que le hizo perder alrededor de 2 millones de euros en criptodivisas. El gran error que cometió, fue guardar en un texto plano de la aplicación Evernote (diseñada para gestionar notas del día a día) todas las contraseñas de sus cuentas relacionadas con las criptomonedas, haciendo la tarea del hacker mucho más sencilla.

En numerosas ocasiones, al hablar de ciberseguridad, el discurso se centra en las contraseñas, pero existen muchos otros riesgos que están provocados por una mala actuación o concienciación del usuario. La conexión a redes wifi abiertas desconocidas, la utilización de herramientas no diseñadas para el tratamiento de datos sensibles, la instalación indiscriminada de aplicaciones no seguras o con permisos excesivos o el almacenamiento sin control de discos extraíbles son cuestiones con un impacto similar o superior a las contraseñas.

Aunque bien es cierto que todas estas prácticas pueden ser programadas en gran parte para evitar riesgos innecesarios, la formación y concienciación del usuario son puntos clave para proteger la seguridad de las aplicaciones y equipos.

Dicho lo anterior, existen algunos casos en los que la actividad del usuario hace que las medidas implantadas dejen de tener efecto y sea un trabajo en balde. Un ejemplo claro, es que, tras la configuración de un acceso robusto a las plataformas corporativas, los empleados tomen como práctica anotar sus contraseñas en pósits que dejan al lado de los equipos. En este escenario, por muy efectiva que haya sido la solución técnica, el usuario final, por su falta de información o de concienciación, ha creado un riesgo adicional que antes no existía.

A nivel normativo, normas como el RGPD (dentro de los deberes del delegado de protección de datos) así como las diferentes normativas de normalización como puede ser la serie ISO 27000, así como la norma UNE 19601 ya recogen la necesidad de formación y concienciación del personal de la empresa en estos aspectos.

Dentro de este terreno normativo, y a la hora de una justificación de la correcta implantación de este tipo de sistemas, el desarrollo de actividades de formación y concienciación de los usuarios es un punto a tener en cuenta

La ciberseguridad, está en el día a día de las organizaciones y debe existir una concienciación al respecto. Un sistema de gestión de la seguridad de la información bien estructurado además de tener unas medidas técnicas y organizativas férreas, debe hacer énfasis en la formación y concienciación de los usuarios. Así las cosas, y por desgracia en demasiadas ocasiones, el usuario pasa de ser la última línea de defensa a ser el principal origen de los riesgos relacionados con la ciberseguridad.

---

[1] https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf