<< NOTICIAS DE SEGURIDAD INFORMÁTICA >>

www.scprogress.com

Teoría y práctica en la seguridad de las contraseñas

El departamento de psicología de la Universidad del Estado de Wichita ha publicado un estudio sobre el uso de las contraseñas en Internet. En el título ya queda claro una de las conclusiones que pueden desprenderse de la encuesta: "La seguridad de las contraseñas: Lo que los usuarios saben y lo que realmente hacen", dejando entrever que existe una discordancia manifiesta entre lo que saben que puede resultar inseguro y lo que realmente hacen. Sin duda, prima la comodidad frente a la eficiencia.

El estudio, conducido por Shannon Riley para "Usability News" en su número de febrero, investiga las prácticas reales de generación y mantenimiento de contraseñas de un grupo de 315 universitarios. Como era de esperar, los resultados evidencian que en general, los usuarios no modifican la complejidad de las contraseñas según el lugar para el que sean usadas (protegen de igual forma su contraseña del banco que la de su sala de chat preferida) ni tampoco las modifican cada cierto tiempo además de usar palabras relacionadas personalmente con ellos. Nada nuevo, excepto que, según responden en la misma encuesta, al menos reconocen que su "política de contraseñas" está lejos de ser la ideal. Entre la teoría la práctica se abre un largo trecho.

Los datos concretos sobre la encuesta (realizada a través de un test de 101 preguntas) no deja lugar a dudas. Los participantes (entre 18 y 58 años, con una media de 25 y todos usuarios habituales de Internet) utilizan reglas simples para generar sus contraseñas. Un 35% usaban un número predeterminado de caracteres en sus claves, con una media de 6.84 caracteres. Una contraseña puede considerarse "fuerte" a partir de los 8 caracteres de longitud.

El 75% afirmaba tener un conjunto predeterminado de contraseñas que usan frecuentemente. De ellos, casi todos (98.3), tenían una media de 3 contraseñas para todas sus actividades en Internet. Casi el 60% afirma no modificar la complejidad de sus claves al usar distintos servicios de la red.

Los usuarios mantienen su contraseña durante una media de dos años y siete meses. Esto en el caso de que las cambien, pues más de la mitad (52%) nunca lo hacen. El 85.7 sólo utiliza letras minúsculas para sus contraseñas, y el 56.5% lo combina con números. Además, el 55% confiesa utilizar palabras cercanas a su entorno (nombres de hijos, mascotas, nombres de calles, de ídolos...) y el 50% sólo números que sean significativos para ellos (teléfonos, fechas de nacimiento...). El 54.6% utiliza la misma contraseña para muchas cuentas y servicios distintos en Internet.

Hasta aquí, nada que no sepamos ya: la mayoría de los usuarios utiliza contraseñas débiles. Lo curioso llega en el apartado de las preguntas destinadas a determinar si los usuarios, al menos, conocen cuáles serían unas buenas prácticas de seguridad ante el uso de sus contraseñas. El 73% sabe que debería cambiarlas al menos una vez cada seis meses (pero el 52% nunca lo hace). Aproximadamente la mitad sabe que debería combinar caracteres distintos y especiales en sus claves, pero sólo el 4.8% lo hace. El 63.5% sabe que sus claves deberían poseer una longitud superior a siete caracteres, pero sólo el 35% usa claves de este tipo. Aproximadamente el 70% sabe que no se deberían utilizar contraseñas que representen palabras o números que signifiquen algo para su dueño, pero más de la mitad mantiene esta práctica.

Ante estos datos, cabe preguntarse dónde está el error. Siempre se habla de la formación y educación de los usuarios en materia de seguridad y al menos en este estudio sobre una población determinada, supuestamente universitaria (aunque pertenecientes a una comunidad homogénea) parece que a base de repetir consignas, los usuarios conocen la teoría sobre seguridad de las contraseñas. El único problema es que no la ponen en práctica, quizás por suponer un esfuerzo que no están dispuestos a realizar. Recordar contraseñas complejas y distintas para muchos servicios en la red se les antoja una tarea complicada que no merece la pena. Probablemente piensen que no se corre tanto riesgo como para necesitar una organización compleja de contraseñas, que nunca serán objetivo de atacantes ni supondrá un problema mayor que alguien distinto a ellos conozca su clave personal.

Teniendo en cuenta lo que las empresas y páginas en general invierten en infraestructuras de seguridad, resulta irónico que sean los propios interesados los que aporten el eslabón débil de la cadena. Es mucho más sencillo deducir o adivinar una contraseña de un usuario que intentar robarla por algún medio tecnológico medianamente sofisticado. Son los propios usuarios los que usan llaves sencillas para proteger su intimidad e intereses en lugares que intentan protegerla con medios técnicos.

Lo interesante pues, consiste en ofrecer técnicas prácticas para conseguir una buena política de seguridad con las contraseñas, en vez de machacar la cansina teoría que ya conocen pero no utilizan. Por ejemplo, hoy en día, cuando es barato y popular el uso de medios de almacenamiento portátiles (tales como llaves USB o reproductores MP3) y también se necesitan distintas contraseñas para todo, es cuando los usuarios lo tienen más sencillo para plantearse el uso de programas de almacenamiento y gestión segura de múltiples contraseñas (tales como el excelente Password Safe). De esta forma podrían llevar con ellos siempre un archivo cifrado con una contraseña fuerte (la única que deberían recordar) que contenga el resto de claves. Así, como si de una pequeña caja fuerte se tratase, podrían disponer a través de una llave maestra de otras contraseñas seguras sin necesidad de recordarlas o apuntarlas en ningún lugar.

Si el hecho de usar contraseñas débiles y repetidas es cuestión de desidia y comodidad, estudiar y llevar a cabo alternativas prácticas muy

eficaces para protegernos puede resultar incluso más sencillo... sólo es cuestión de conocer esas alternativas (no sólo la teoría) y querer aplicarlas.

Más Información:

Password Security: What Users Know and What They Actually Do
http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm

Password Safe
http://passwordsafe.sourceforge.net

NOTA

1. Ponemos a consideración el servicio de e-learning para capacitarse en algunos temas que pueden ser de interés para ustedes.

   http://www.scprogress.com/moodle/

2. Por favor háganos conocer si estaría Usted interesado en seguir un curso de seguridad informática a través de e-learning, con instructores de reconocido prestigio.

   Ing. Arturo de la Torre