ASR Ltda.

NOTI INFORMATIVO

FEBRERO DE 2014

EDICIÓN No. 223

SEGURIDAD EN LOS SISTEMAS: SIMPLE O COMPLICADA

Siempre que se mencionan fraudes en Sistemas, se tiene la idea mental de un grupo de hackers, personas altamente competentes y geniales, capaces de vulnerar todos los sistemas de protección existentes en las organizaciones. En las películas vemos a jóvenes con obvios problemas de falta de habilidades sociales, trabajando de forma frenética en varios teclados al tiempo, mientras observan pantallas con gráficos extraños.

La realidad nunca puede estar más alejada de la ficción como en este caso. En la vida diaria, los peores fraudes por computador los cometen personas con elementales conocimientos de su uso, quienes en cambio son hábiles para descubrir y explotar las debilidades de los usuarios de los sistemas, o de los procedimientos diseñados para su utilización en las empresas.

No hay que ser un genio para apoderarse de la clave de acceso de un compañero de trabajo, especialmente cuando éste no tiene problema en dejarla anotada en un papel sobre su escritorio. No se necesita ser brillante para insertar una memoria externa en un computador ajeno que ha sido dejado sin vigilancia, y copiar los archivos que allí estén contenidos.

Casi todos los casos de fraude por computador incluyen violaciones ingenuas a las más elementales medidas de seguridad para su manejo. Nos permitimos sugerir algunas medidas de fácil aplicación, para disminuir la vulnerabilidad de las empresas frente a este tipo de fraudes:

- Claves de acceso: las claves de acceso deben estar constituidas por al menos 8 caracteres, entre los que se incluyan una letra mayúscula, un número y dos símbolos;

- Cambie las claves a intervalos regulares. Una clave que nunca se cambia termina siendo conocida por muchas personas;

- Para evitar el riesgo de pérdida de información, implemente una política de destrucción de todos los

documentos que salgan de la empresa. Ello evitará que información sensible caiga en manos equivocadas;

- No descuide los discos duros. La información confidencial almacenada en estos discos es el principal objetivo de los delincuentes. El simple borrado no es suficiente. Tenga en cuenta que la única forma de borrar de manera permanente un archivo, es destruyendo físicamente el disco duro;

- Adecúe lugares seguros para almacenar la información sensible. Los documentos restringidos permanecen al alcance de muchas personas sobre los escritorios. Asegúrese que dichos documentos queden bajo llave, cuando el responsable de ellos se ausente de su puesto de trabajo;

- Destruya antes de donar o reciclar. No deje intactos en los tarros de basura los documentos sensibles que hayan sido descartados. Recurra a empresas serias y supervise el proceso de destrucción. Destruya los discos duros en desuso;

- Sensibilice. Debe crearse y fomentarse una cultura de protección de la información entre sus empleados, que les permita entender la importancia de proteger el recurso información. Audite de manera regular el cumplimiento de las normas de seguridad adoptadas;

- Piense en la prevención, no en la reacción. Es mucho más costo beneficioso prevenir que tener que gastar tiempo y esfuerzos en manejar las crisis derivadas de los eventos de fuga de información. Estrategias que van a la raíz de los procesos y que consideran la totalidad del ciclo de vida de la información (desde que se genera y almacena hasta que se destruye), permite contar con mejores modelos de manejo de este riesgo.

Estamos seguros que estas pequeñas recomendaciones ayudarán a mejorar la seguridad en el manejo de uno de los más valiosos activos de toda organización.

asr@asr.com.co