¿Se pueden robar tus claves de acceso secretas y arruinar archivos de información? Un análisis en los sistemas de Información contable.

Diego Sebastian Escobar.

APLICACIÓN DE HERRAMIENTAS DE LA SEGURIDAD INFORMÁTICA EN LOS SISTEMAS CONTABLES PARA MITIGAR LOS RIESGOS DE FRAUDES Y SABOTAJES INFORMÁTICOS.

¿SE PUEDEN ROBAR TUS CLAVES DE ACCESO SECRETAS Y ARRUINAR ARCHIVOS DE INFORMACIÓN?

Expositores: Dra. Elsa Beatriz Suarez Kimura
Contador Público y Maestrando en Seguridad Informática
Diego Sebastián Escobar

¿Se pueden robar tus claves de acceso secretas y arruinar archivos de información? Un análisis en los sistemas de Información contables.

Diego Sebastián Escobar
Becario de Maestría UBA
Contador Público – Maestrando en Seguridad Informática
Centro de Modelos Contables – FCE - UBA

¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

- La Real Academia Española establece que seguridad, es la cualidad de Seguro, es decir estar libre y exento de todo daño peligro o riesgo. En tecnología de la información, la seguridad entendida según la citada definición es prácticamente imposible de conseguir, "*por lo que se tiende mas al concepto de fiabilidad*"; entendiéndose a un sistema seguro como aquel que se comporta como se espera de él.

1- Julio Gómez López, "Guía de campo de hackers", Capítulo I,. México, 2010, Alfaomega Grupo Editor. 17 p

Principios de la Seguridad de la Información	
Confidencialidad	**Requiere que la información sea accesible (usarla, leerla o escucharla) a las personas autorizadas.**
Integridad	**Requiere que la información sólo pueda ser modificada por las entidades autorizadas. Asegurando que la información con la que se trabaja sea completa y precisa, poniéndole énfasis en la exactitud tanto en su contenido como en los procesos involucrados en su procesamiento.**
Disponibilidad	**Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando se los necesiten.**
Fuente: Elaboración Propia	

¿Como se almacenan las Claves en un Sistema Operativo?

- Texto Plano.

Si el archivo es comprometido, **todas** las claves lo Están

- Texto Cifrado.

Necesita claves para cifrado/descifrado en memoria terminamos en problema anterior

- One-way Hash de la clave.

Si el archivo es comprometido, el atacante aún debe adivinar las claves o invertir la función.

Ejemplos de Ataques

- Ataques de Diccionario
- Ataques de fuerza Bruta

Almacenamiento de claves de usuarios.

Mecanismo utilizado en Windows

Lan Manager Hash

- Se convierte todo a mayusculas antes de generar el hash.
- La clave se divide en dos bloques de 7 caracteres, antes de aplicar el hash. Si la clave tiene menos de 14 caracteres, se paddea con null.
- Utiliza DES, encriptando con la clave el texto KGS!@#$%”
- El resultado del hash es un valor de 16 bytes.
- No se utiliza Salt.

Experimento

Elección de claves y otros sistemas

- Selección aleatoria
- Claves pronunciables
- Claves elegidas por los usuarios

- - Otros Sistemas de autenticación:
- Biométricos
- Tokens
- Etc.

Ejemplos:

¡¡¡Muchas Gracias!!!

Centro de Modelos Contables – FCE - UBA