UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE CONTADURIA PÚBLICA
AUDITORIA DE SISTEMAS

TALLER SOBRE CONTROLES

Para los siguientes casos establezca como mínimo 3 controles:

1. COMPUTADOR UTILIZADO PARA FRAUDE

Un antiguo operador de computador del Depto de Ayuda Pública de los Estados Unidos y otras tres personas fueron procesadas por un juez por haber defraudado el departamento por US$73.525

El proceso señala que un computador en las oficinas del departamento fue programado para emitir cheques de beneficio no autorizados.

El abogado de la Corte Estatal, Bernard Carey, dijo que 173 cheques no autorizados, cada uno por US$425, fueron emitidos y cobrados durante un período de seis meses, el cual terminó en diciembre último.

Los procesados son: Annie Quinn de 28 años, operadora de computador que fue cancelada de su empleo en el departamento de Beneficios en el mes de febrero, luego que el plan fue descubierto; Van Strickland de 25 año, instalador de la compañía telefónica y acusado de ser el autor intelectual del plan, y dos beneficiarios: Carol Powell de 25 años y Roberta Jackson de 25 años.

Carey dijo que el caso todavía está en investigación y se rehusó a decir si habían otros beneficiarios envueltos.

Se supo que en el reparto de los cheques de US$425, Strickland había recibido US$200, Miss Quinn US$100 y los beneficiarios cómplices US$125.

Esto significa que durante un período de seis meses Strinckland recibió US$34.600, Miss Quinn US$17.300 y los beneficiarios un total de US$21.625 entre los dos.

Los investigadores afirman que Strickland reclutó a los beneficiarios ofreciéndoles dinero fácil a cambio de la aceptación por parte de ellos de repartir la mayor parte de cada cheque después de cobrarlo.

Los beneficiarios recibieron los cheques no autorizados de US$425 además de los cheques de ayuda pública regulares.

Carey informó que el Director Financiero del Departamento de Ayuda Pública, descubrió el plan durante una auditoría, pues le llamó la atención el que hubiera un gran número de cheques de US$425, ya que la mayoría de los cheques en esta categoría de beneficiarios es solamente de US$350.

Los investigadores del departamento de Ayuda Pública y los abogados del Estado trabajaron durante cinco meses para reunir los detalles del plan para presentarlo al gran jurado.

Un fraude en el programa de beneficios, que es de US$1.600 millones por años, es un problema común y actualmente es el centro de una amplia investigación por parte de un gran jurado federal.

2. TRANSACCIONES DE VHS PONE AL DESCUBIERTO PLAN DE ROBO DE MERCANCIAS

Cuando trabajaban secretamente en un caso de drogas, agentes del IBI descubrieron que la manipulación de un sistema computarizado de manejo de mercancías en una compañía local de ventas al por mayor llevó al robo de algunas mercancías por valor de US$20.000

El agente del IBI dijo que había acabado de comprar algún VHS al jefe de embarque de la Compañía EBY-BROWN, cuando el mismo comenzó a contarle sobre los beneficios de "saquear la compañía" con el robo de televisores, estéreos y otras mercancías.

Creyendo en las "fanfarronadas" del jefe de embarque, el agente alertó a los directivos de la EBY-BROWN

Las investigaciones iniciadas levantaron sospechas sobre un operador de computrador del turno de la noche quien podía manipular el sistema de existencias mientras trabajaba solo.

Analizando los reportes emitidos en ese período, los agentes descubrieron números de facturas duplicados conteniendo mercancías diferentes.

Investigaciones más detalladas llevaron a la conclusión de que a través del sistema el operador, antes de totalizar una factura, alteraba ciertos números de factura incluyendo y/o sustituyendo códigos y valores que se reflejarían en un crédito de venta para la mercancía que había sido robada.

El plan envolvía también la manipulación del "Reporte de Registro de Ventas" el cual contiene información sobre los pedidos pendientes, ventas anuales, ventas a la fecha y las ventas de la semana.

Aparentemente el operador también utilizó la técnica de disminuir las cantidades de algunos artículos recibidos, a fin de seleccionar las mercancías a ser robadas.

Una tercera técnica utilizada consistía en cancelar el inventario de artículos colocados previamente fuera del lugar normal de almacenamiento y embarque.

EBY-BROWN admitió que fue negligente por no mantener un severo control de inventario, y como el monto de lo robado no era suficientemente grande para levantar una sospecha, no había percibido nada.

3. FALTA DE CONTROL EN CINTOTECA

La señorita SUSY, responsable de la Cintoteca de un Centro PED, supo con un buen tiempo de anterioridad que había sido despedida de la organización.

SUSY sabía que las cintas de respaldo enviadas por ella misma al lugar de seguridad, fuera de la entidad, como protección contra posibles desastres, no serían usadas, a menos que se presentaran problemas en los archivos respaldados. Ante esta situación, SUSY decidió sustituir las cintas de respaldo de los archivos maestros por cintas en blanco o de borrador y cambió las etiquetas externas.

Después de unos días, cuando ella estuvo segura de que era prácticamente imposible reconstruir los archivos maestros sin el auxilio de los Back-up correspondientes, entonces borró muchos de los archivos críticos que se encontraban en la cintoteca y se retiró de la entidad.

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE CONTADURIA PÚBLICA
AUDITORIA DE SISTEMAS

FRAUDES RELACIONADOS CON EL COMPUTADOR

1. **DEFINICION:** El fraude es un acto intencional que impacta los activos de la empresa porque hay hurto; encubrimiento de obligaciones o deudas, y/o manipulación de ingresos y gastos. Cuando se tiene un computador implicado en el acto de fraude, se habla de fraude electrónico, fraude por computador o fraude informático.

2. **CONCEPTO DE FRAUDE INFORMATICO**: El fraude informático referencia a cualquier desfalco perpetrado mediante el uso indebido y/o adulteración de: Archivos de Datos, Entrada de Datos, Hardware, Líneas de Comunicación, Salida de Datos, Software de Aplicación, Software Operativo, etc.

3. METODOS DE FRAUDE RELACIONADOS CON EL COMPUTADOR

3.1 ADULTERACION DE DATOS: Es la maniobra más utilizada. Consiste en cambiar los datos antes o durante la entrada de éstos al computador. Puede ser realizada por cualquier persona que tenga acceso a los procesos de creación, registro, transporte, codificación, verificación, o conversión de datos.

3.2 ATAQUES ASINCRONICOS: Esta técnica radica en tomar ventaja del funcionamiento asincrónico del sistema operacional. El sistema no ejecuta los trabajos en el mismo orden en que son recibidos, sino que los ejecuta asincrónicamente basado en la prioridad del trabajo y en la disponibilidad de recursos. Así, hay métodos que permiten usar el sistema operacional para violar el aislamiento entre un trabajo y otro y lograr acceso no autorizado o modificación de los datos.

3.3 BOMBAS LOGICAS: Estriba en colocar instrucciones ilícitas dentro de un programa inofensivo para ser activadas cuando se cumpla una condición o estado específico. Mientras no se satisfaga la condición, el programa se ejecuta de manera apropiada. Cuando la condición o estado especificado es satisfecho, automáticamente se activa la rutina que ejecuta la acción no autorizada.

3.4 CABALLO DE TROYA: Consiste en insertar mandatos ilegítimos dentro de un programa, de manera que además de las funciones propias del programa, también se ejecuten funciones no autorizadas. Las instrucciones fraudulentas se esconden dentro de las demás instrucciones, logrando acceso libre a los datos que normalmente son usados por el programa. Estos mandatos ilegítimos también pueden ocultarse dentro del sistema operacional o los programas de utilidad. Preferencialmente son introducidos adicionando un cambio no autorizado, en el momento en que se realiza un cambio autorizado.

3.5 EVASIVA ASTUTA: Método inventado a raíz de la aparición de los compiladores. Los programadores del sistema lo inventaron para meterse en el computador, cambiar las cosas, hacer que suceda algo y volver a la forma original, todo ello sin dejar huella.

3.6 HURTO COMUN: Consiste en el simple robo de dispositivos de almacenamiento de información tales como cintas magnéticas, diskettes, etc., por personas que han tenido acceso a esos elementos eludiendo controles existentes.

3.7 INGENIERIA SOCIAL: Estriba en conmover, sobornar o extorsionar a quienes pueden entregar la información deseada o a quienes pueden facilitar la consumación de ilícitos.

3.8 INTERCEPCION DE LAS LINEAS DE COMUNICACIÓN: Radica en una conexión secreta activa o pasiva, en los circuitos de comunicación telefónica y/o telegráfica entre terminales y concentradores; terminales y computadores, o computadores y computadores, para interceptar mensajes.

3.9 JUEGO DE PIZZA: Es un método fácil para lograr acceso a áreas de cómputo estrechamente controladas. Un individuo se hace pasar por el mensajero que entrega las pizzas. Este disfraz garantiza que el sujeto tenga acceso inmediato al área y después de la jornada normal de trabajo.

3.10 PARCHEO: Reside en usar programas de utilidad que permitan actuar sobre los datos de los archivos o las instrucciones de los programadas almacenados, modificándolos a pesar de que se encuentren protegidos por claves de seguridad.

3.11 PYGGYBACKING (IR A CUESTAS): Consiste en el hurto de contraseñas, claves o llaves con el fin de realizar un ilícito. Este robo generalmente es efectuado por individuos que se ubican detrás de las personas poseedora, con el objeto bien de apropiarse de la llave o de memorizar la clave o la contraseña, para así tener acceso a una máquina o área de acceso restringido.

3.12 PUERTAS LEVADIZAS: Se basa en el concepto que se utilizaba en las fortalezas amuralladas donde el acceso era controlado por los moradores mediante puertas levadizas. Consiste en construir puertas levadizas mediante rutinas en los programas de computador o colocando en la unidad central de proceso transmisores miniaturas u otro tipo de hardware, para permitir que los datos entren y/o salgan controlados desde adentro.

3**.13 RECOLECCION DE BASURA:** Consiste en buscar copias abandonadas de los listados de computador, papel carbón, datos residuales dejados en el computdor o cualquier otro elemento que permita conocer la información relacionada con los programas de computador o con las operaciones de la empresa.

3.14 SUPERZAPPING: Deriva su nonmbre del Superzap programa utilitario de la IBM que permite adicionar, modificar o eliminar registros sin tener que utilizar los programas normales de aplicación usados para manejar y mantener los archivos de datos.

3.15 TECNICA DEL SALAMI: Radica en robar pequeñas sumas o cantidades (tajadas) de los registros de datos mediante rutinas incrustadas en los programas de aplicación.

3.16 TECNICA DEL TALADRO: Estriba en hacer llamadas desde un computador casero mediante ensayos permanentes hasta lograr el acceso en un sistema computarizado. Se utiliza para descubrir las contraseñas de acceso a terminales.

3.17 TRAMPAS PUERTAS O AGUJERO: Son deficiencias en los diseños de los computadores y sus sistemas operacionales. Expertos programadores pueden sacar ventaja de esas puertas para insertas códigos adicionales y realzar funciones no autorizadas. Existen muchos agujeros que permiten al perpetrador sin que éste sea un experto programador, cometer fraudes. Por ejemplo, las salidas de programas del sistema operacional que permite transferir el control o programas escritos por el usuario.

3.18 UTILIZAR LA APATIA DEL USUARIO: Muchos usuarios están convencidos que sí lo hizo el computador debe estar correcto o que los errores desaparecen con el tiempo. Este convencimiento puede ser utilizado por el programador para cometer ilícitos.