www.eysglobal.com

ESTUDIO DEL CASO
PARTE 2

RECORDEMOS DEL PROBLEMA

La empresa de salud VIDA SANA tiene dentro de sus funciones entregar el medicamento a los usuarios, en la auditoría realizada se encontraron anomalías en la droguería de la empresa en cuanto a la compra de medicamentos y despacho de las mismas a los usuarios.

ESTUDIO DEL CASO PARTE 2

4. CRITERIOS USADOS PARA LA BÚSQUEDA DE EVIDENCIA

Para el caso de elementos encontrados en el entorno físico:

- Explorar todo el contorno y lugares aledaños al sitio donde ocurrieron los hechos delictivos.
- Inspección ocular a los dispositivos encontrados en el lugar.
- Inspección a las conexiones de los equipos o dispositivos aledaños al sistema informático vulnerado.
- Indagación a personal propio de la organización, es recomendable hallar
- individuos confiables que suministren información.
- Buscar, documentar, describir y conservar las huellas que pueden servir para lograr dilucidar lo ocurrido.

ESTUDIO DEL CASO PARTE 2

- Buscar personal adicional experto en registro fílmico, auditivo, digital y/o documental para que ayude a solucionar el rompecabezas de la escena del crimen.
- Registrar las dimensiones del lugar o lugares involucrados en el hecho delictivo.
- Determinar mediante hipótesis el modus operandi del delincuente.

Para el caso de la información digital encontrada en los dispositivos investigado

- Los archivos de sistema modificados tras la instalación del sistema operativo.

ESTUDIO DEL CASO PARTE 2

- Averiguar la ubicación de los archivos ocultos, de qué tipo son identificar también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por los atacantes, destacar la importancia de realizar imágenes de los discos pues se puede acceder al espacio residual que hay detrás de cada archivo, (recordar que los ficheros suelen almacenarse por bloques cuyo tamaño de clúster depende del tipo de sistema de archivos que se emplee), y leer en zonas que el sistema operativo no ve.
- Pensar que está buscando “una aguja en un pajar”, por lo que se deberá ser metódico, ir de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

ESTUDIO DEL CASO PARTE 2

Comenzar a examinar con más detalle los ficheros logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una correlación temporal entre eventos. Pensar que los archivos logs y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que tendrá que buscar entradas extrañas y compararlas con la actividad de los ficheros. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el ataque del sistema.

ESTUDIO DEL CASO PARTE 2

- La extracción de información se puede realizar por diversos medios teniendo en cuenta que los más utilizados son medios ópticos, extraíbles USB, correo electrónico, almacenamiento externo como DropBox y otros.
- La alteración de los precios en la compra y despacho de los medicamentos y registro de la factura de compra.
- Entrega a los pacientes más de los medicamentos formulados, para con esto justificar las compras extras de reservas.
- El hacer compras ficticias para hacerse a esos dineros extras.
- La verificación si el fraude se realizó durante el receso de algunos funcionarios para ser implicados en el ilícito.

ESTUDIO DEL CASO PARTE 2

- La alteración y modificación de los datos en las bases de almacenamiento sobre el inventario reservado como el adquirido recientemente.
- Revisión de los correos de los empleados donde se encuentra almacenada información que puede ser tenida en cuenta para la auditoría y los cuales se encuentran en un sistema sobre el que no se tiene control directo (por ejemplo gmail, Hotmail, etc.).
- Por desgracia para los implicados en el fraude, los proveedores guardan copia de sus facturas sobre los productos entregados a la empresa de salud.

ESTUDIO DEL CASO PARTE 2

EVIDENCIA

1. QUE ESTRATEGIAS SE USARON PARA LA RECOLECCIÓN DE PRUEBAS ELECTRÓNICAS

Llevar un orden de recopilación de información
Este aspecto permite que el análisis y posteriores hallazgos en el proceso investigativo forense para el caso de la empresa de salud VIDA SANA, sea realmente valido, preciso, conciso y veraz. Un orden en el proceso permite que los resultados sean contundentes y satisfactorios, la justicia dará credibilidad a la investigación forense y análisis llevado a cabo, por ende la ley se aplicará de acuerdo a los delitos impugnados al o los atacantes.

ESTUDIO DEL CASO PARTE 2

Buscar la evidencia: Para esta actividad se hace necesario establecer previamente las evidencias a tener en cuenta para su recolección, esto es; mediante un listado de registro detallar las objetos, medios de información, aspectos del entorno entre otros factores que ayuden a establecer con certeza todo lo que se está buscando y espera encontrar para dar más contundencia a la investigación forense.

ESTUDIO DEL CASO PARTE 2

Determinar la relevancia de los datos: En este aparte se hace necesario tener un cierto grado de conocimiento, experiencia y experiencia por parte del perito o investigador forense, dado que en cualquier caso delictivo informático; existe en la escena del crimen/fraude, elementos probatorios de mayor relevancia pertinentes a la investigación o como también pueden existir otros que se pueden considerar útiles, pero no necesarios de incluir en el proceso investigativo, pues; carecen de valor probatorio.

ESTUDIO DEL CASO PARTE 2

Determinar la volatilidad de la información: Todo dispositivo de almacenamiento electrónico se considera volátil, pues; la información puede estar presente allí y almacenarse, y en determinado momento puede ser alterada, modificada o borrada de dicho dispositivo.

Es importante tener en cuenta que para recolectar la información contenida en estos dispositivos, se debe contar con un procedimiento formal que establezca el orden de prioridad con que esta se debe recolectar para no cometer errores en la investigación. Estos errores pueden hacer que la información allí presente en estos medios de almacenamiento en un determinado instante desaparezca, haciendo que el posterior proceso de análisis pierda elementos claves y necesarios que permitirán realizar hallazgos contundentes en la investigación.

ESTUDIO DEL CASO PARTE 2

Eliminar la interferencia exterior: En este punto es importante recalcar que factores externos al proceso investigativo, pueden afectar considerablemente los resultados esperados. Si un elemento probatorio o evidencia es contaminada, se pierde la integridad de esta y por ende la credibilidad y validez ante la justicia. Por esta razón el investigador forense ha de identificar con antelación los posibles elementos o factores que pueden afectar de manera directa o indirecta la integridad de la información recolectada junto a los elementos hallados en la escena del delito.

ESTUDIO DEL CASO PARTE 2

Recoger la evidencia: Tras haber obtenido los elementos probatorios o evidencia a tener en cuenta para el proceso investigativo, se hace necesario que estos sean recolectados usando metodologías o procedimientos acordes a la conservación idónea de estos, por esta razón necesario acudir al uso de herramientas que de aquí en adelante harán parte integral de la cadena de custodia, entre estas; se tiene el uso de embalajes a base de papel , como sobres de papel manila y cajas de cartón, que permitirán almacenar los documentos físicos que contienen información importante, relevante y adicional que ayudarán a fundamentar con mas contundencia los hallazgos o hipótesis en la investigación.

ESTUDIO DEL CASO PARTE 2

Documentar todas las acciones realizadas: Para este paso se recomienda el documentar muy detallada y minuciosamente los pasos, procedimientos y labores realizadas en el proceso de investigación forense, pues; cualquier paso en falso o falta de validez en una prueba presentada ante el o los jueces, puede terminar arruinando el trabajo realizado y por ende el terminar el proceso con resultados negativos. El uso de una bitácora de trabajo elaborada por el investigador, el uso de cámaras fotográficas, las marcas de tiempo, las firmas digitales, y las declaraciones firmadas sirven para ayudar a validar de manera contundente el proceso investigativo.

ESTUDIO DEL CASO PARTE 2

2. QUE INDICIOS FUERON TENIDOS EN CUENTA PARA LA RECOLECCIÓN DE EVIDENCIAS.

- Alteración en los precios de compra de los medicamentos en el sistema de administración y entrega de medicamentos.
- Modificación en bases de datos del stock o inventario de medicamentos sin la debida autorización.
- Uso de memorias USB para la extracción de información sensible almacenada en los computadores para ser analizada al exterior de la empresa.
- Alteración en los soportes de compra y valores entregados por los proveedores.
- Facturación de medicamentos realizada con precios inflados a los ofrecidos por los proveedores.

ESTUDIO DEL CASO PARTE 2

- Alteración de datos en las autorizaciones de entrega de los medicamentos a los pacientes.
- Reuniones a puerta cerrada en la escena del delito por parte de los funcionarios y que fueron grabadas en audio y vídeo por el circuito cerrado de seguridad de la empresa mediante cámaras de vigilancia.
- Envío de email o correos a otros presuntos involucrados en el fraude.
- La entrega a los pacientes de más de los medicamentos formulados, para con esto justificar las compras extras de reservas.
- Las diferencias encontradas en las órdenes entregadas de medicamentos a los pacientes, las cuales no correspondían con los registrados en las copias expedidas por los médicos que atendieron a los respectivos pacientes.

ESTUDIO DEL CASO PARTE 2

3. CUIDADOS TENIDOS EN CUENTA AL TENER EVIDENCIA VOLÁTIL

- Se realizó copia de seguridad o backup, a cada uno de los discos duros de los equipos que se guardaron para el análisis de la información que se encuentra almacenada para su respectiva verificación.
- Se reservó el ingreso de personal que labora en el centro de salud, para lograr privacidad y movilidad en todas las secciones implicadas en las que se detectó el fraude y alteración de la información por la cual se encontró el ilícito.
- El resguardo en lugar seguro de los dispositivos móviles solicitados e implicados en el fraude.
- La protección a los archivos en los que se digitaron las identificaciones o autenticaciones respectivas, que fueron solicitadas al personal a los cuales se les realizará la respectiva investigación referente al fraude detectado en la empresa de salud.

ESTUDIO DEL CASO PARTE 2

. ANÁLISIS DETALLADO A LA EVIDENCIA RECOLECTADA

- Se analiza la información detallada a cada una de las copias de las órdenes de medicamentos que fueron entregadas a pacientes afiliados al centro de salud “VIDA SANA ”, con el fin de ratificar la sobre medicación y entrega excesiva de fármacos a éstos por parte de los encargados de la farmacia.
- La exploración detallada y pormenorizada de las carpetas contenidas en los Discos Duros de los computadores para encontrar información o archivos ocultos que serán encontrados y tenidos en cuenta para la investigación de la negociación entre funcionarios y proveedores de medicamentos.

ESTUDIO DEL CASO PARTE 2

- realizar una cuantificación de existencias basándose en el inventario actual en comparación a los productos solicitados que fueron comprados a proveedores implicados en el fraude.
- La realización de la investigación detallada de la participación de cada uno de los implicados en el fraude económico a la entidad, caracterizado y clasificado por los autores intelectuales y materiales que participaron en el fraude, y si se presentó descuido o negligencia por parte de la gerencia que permitió la situación del fraude.
- Entablar un denuncio o demanda de Tipo legal respecto al delito perpetrado por los implicados en el fraude por adulteración en los precios entregados por el proveedor de medicamentos y los precios autorizados por la empresa de salud.

ESTUDIO DEL CASO PARTE 2

CONCLUSIONES

- Se logró identificar las etapas de la ciencia forenses en tecnológica que se deben aplicar para adelantar una investigación forense.
- Se identificó los procedimientos a implementar para asegurar la escena de los posibles hechos delictivos.
- Se reconocieron los procesos para asegurar la evidencia que objeto de investigación.
- Se encuentra que es posible realizar una búsqueda de evidencia tanto física como circunstancial para la comprobación del fraude, bien sea de tipo informático o de cualquier otro tipo de delito cometido dentro de una organización o entidad.

ESTUDIO DEL CASO PARTE 2

- El cuidado que se debe tener con la información encontrada de tal forma que no sea perdidiza con facilidad y contar con la honestidad del ente investigador que se encuentra realzando la investigación respectiva y por el cual fue contratado.
- Esclarecer el tipo de seguridad para los activos de información, responsabilidades y planes de contingencia, priorizando lo que se debe proteger y como se realizará a protección debida a cada evidencia.
- La realización de respaldo periódicamente de los datos a los que deben realizar copias de seguridad para su posterior restauración, en caso de pérdida o corrupción de los datos, así como el manejo y control de los virus e intrusos, estableciendo políticas de seguridad ante la presencia de malware y spyware, evitando al máximo los riegos de intrusión a los sistemas exclusivos que contienen información relevante.

ESTUDIO DEL CASO PARTE 2

- Reconocer la metodología para la extracción de la información la cual se puede realizar por diversos medios, teniendo en cuenta que los más utilizados son medios ópticos, extraíbles como USB y D.D., correo electrónico, almacenamiento externo como DropBox y otros, así como el reconocimiento de la alteración de los precios en las facturas de compra y en las órdenes de despacho de los medicamentos, como el debido registro de la factura de compra.
- Se encontró que se debe realizar un análisis detallado a la información recolectada, de tal forma que se identifique la adulteración de datos y de registros almacenados en las Bases de Datos del sistema de información de la empresa investigada.