Caso 2 – Canales seguros

Cesar Eduardo Quintero Rangel – 201622862

**Análisis y Entendimiento del Problema Considerando el sistema descrito en el párrafo anterior:**

1. Identifique y describa los datos que deben ser protegidos en el sistema de rastreo de unidades de distribución. Explique su respuesta en cada caso y responda la pregunta ¿Si un actor no autorizado consigue acceso al dato mencionado, ya sea en modo lectura o escritura, cómo podría afectar la empresa?

Los datos que deben ser protegidos en el sistema de rastreo deben se lo siguientes:

* Posición de cada una de las unidades de reparto; en caso de que un autor no autorizado pudiera acceder a los datos podría afectar de dos formas diferentes a la compañía: la primera en modo de lectura, podría realizar un seguimiento de las unidades lo cual sería un potencial riesgo para los operarios, junto a ello la competencia podría explotar esos datos (ej. saber en qué puntos geográficos les cuesta más llegar); segundo si se accede con privilegios de escritura, el autor puede hacer creer que las unidades se encuentran en otros puntos diferentes, esto repercutiría en toda la cadena de valor de la compañía.
* Rutas estimadas de las unidades; en caso de que un autor no autorizado consiga acceder a los mismos podría generar varias afectaciones a la compañía, entre las cuales destacan: el potencial seguimiento, riesgo para los empleados, obtención de datos por parte de la competencia y desvió de unidades, todos afectando la operación correcta de la compañía.

Datos a proteger en los demás sistemas informáticos:

* Datos personales de los clientes; generando afectaciones a los usuarios de la compañía, pérdida de confianza y afectaciones legales.
* Datos de las unidades de distribución y los operarios; generar desventaja competitiva y posibles sabotajes por parte de terceros, poniendo en riesgo a todos los empleados de la compañía.
* datos de las ordenes; generando las posibles consecuencias antes mencionadas, adicionalmente en caso de escritura, generando fallos en la distribución y posibles consecuencias adicionales.

2. Identifique cuatro vulnerabilidades de ese sistema, teniendo en cuenta únicamente aspectos técnicos o de procesos (no organizacionales). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento y procesamiento de los datos. Explique su respuesta en cada caso.

* Daños físicos a los servidores; si los servidores se ven afectados ya sea por un fallo energético u otro factor (ya sea ambiental o de manejo interno) podría generar una pérdida total de datos y consecuentemente afectar el funcionamiento interno de la compañía.
* Huecos de seguridad en las configuraciones internas de los servidores; cualquier configuración adicional innecesaria que facilite el acceso a un autor no autorizado a la información protegida por el sistema (ejemplo: juegos, software de edición, software preinstalado, claves por defecto(sistema operativo).
* Seguridad física de los servidores; en caso de que los servidores se encuentren físicamente expuestos a terceros que puedan llegar a afectarlos, (ejemplo: cualquier persona puede insertar un dispositivo USB).
* Caballos de trolla en hardware; en caso de comprar a proveedores no reconocidos se pueden llegar a adquirir dispositivos que a nivel hardware contengan piezas que faciliten la entrada a posibles atacantes (ejemplo: compra de servidores de segunda mano o de marcas poco reconocidas que contengan en su interior una tarjeta de red modificada que envía un duplicado de la información entrante, caches de procesador modificadas, cables, etc…).

3. Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución.

1. Los mecanismos propuestos deben ser explicados. Por ejemplo, si se habla de cifrado sobre un canal de comunicaciones, debe identificar los participantes en la comunicación, y si es cifrado simétrico o asimétrico (y justificar la decisión).
2. Además, debe explicar por qué resuelve la vulnerabilidad identificada

* Daños físicos: dado que no es posible mitigar del todo es te factor se plantea el usar varios servidores que mantenga duplicados de la información, ya que de esta forma se reduce el riesgo de pérdida total, para que la estrategia se a eficiente se debe tener en cuenta que los servidores deben ubicarse en puntos geográficos diferentes, para que de esta forma no se vean afectados en un mismo incidente.
* Huecos de seguridad en las configuraciones: para mitigar esta vulnerabilidad se plantea en cada uno de los servidores el instalar solo en software necesario para la su funcionamiento, adicionalmente se enviaran equipos especializados para que se encarguen de realizar una minimización del área de ataque; junto con lo anterior se plantea la actualización de los servidores con parches de seguridad, primero haciendo las pruebas de funcionamiento necesarias para evitar posibles nuevas vulnerabilidades. Mediante la implementación de las soluciones planteadas se conseguirá reducir el área de ataque.
* Seguridad física de los servidores: se plantea instalar los servidores un área con poca población subyacente, adicional con un sistema de seguridad (guardias, cámaras y procesos de seguridad) que permitan garantizar que ningún tercero no autorizado atendrá acceso a los mismos.
* Caballos de trolla en hardware: se plantea el comprar servidores nuevos de empresas reconocidas, junto con ello el verificar la procedencia de los diferentes componentes por parte de un equipo de seguridad para validar que no se encuentren dispositivos adicionales que puedan afectar su correcto funcionamiento.