Infraestructura Computacional

Caso 2

Juan Carlos Corrales 201531115

Alejandro García Flores 201326489

1. Análisis y entendimiento del problema

Suponiendo que el sistema descrito en el párrafo anterior cuenta con un firewall que filtra paquetes a la entrada de la red y antivirus en todas las máquinas de la compañía:

* 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 lectora o escritura, cómo podría afectar la empresa?
     1. Datos enviados cada 60 segundos entre las unidades de distribución y el servidor que informan el estado de las unidades.
* Modo Lectura: Si un actor no autorizado accede al dato en cuestión en modo lectura, podría conocer el estado actual de la unidad de distribución, violando la confidencialidad de los datos, así como también puede comprometer la seguridad de las unidades de distribución, tales como robos a las unidades de distribución o peor.
* Modo Escritura: Si un actor no autorizado accede al dato en cuestión en modo escritura podría comprometer la integridad de los datos, problemática conocida como Tampering, o suplantar la identidad de una o más unidades de distribución, problemática también conocida como Spoofing comprometiendo la seguridad de las unidades de distribución, dejándolas vulnerables a robos o accidentes por fuera del conocimiento de la empresa.
  + 1. Datos enviados a la 1 am con las rutas que deben seguir las unidades de distribución enviados por el servidor a los clientes.

- Modo Lectura: Un acceso a la información por parte de un actor no autorizado le permitiría conocer las rutas que seguirán las unidades de distribución. Esta es una seria violación de la confidencialidad de los datos, así como también puede comprometer la seguridad de las unidades de distribución, tales como robos a las unidades de distribución o peor.

- Modo Escritura: Un acceso a la información por parte de un actor no autorizado podría comprometer la integridad de la información. Esto es grave debido a que una alteración en las rutas de distribución podría llevar a las unidades por rutas equivocadas y la compañía podría incurrir en gastos adicionales debido a esos errores. También, dependiendo del nivel de automatización de las unidades de distribución, podrían ocurrir accidentes.

* + 1. Datos de excepción cuando un conductor cambia la ruta entre la unidad de distribución y el servidor.
* Modo Lectura: Si un actor no autorizado accede al dato en cuestión en modo lectura, podría conocer el estado actual de la unidad de distribución, violando la confidencialidad de los datos, así como también puede comprometer la seguridad de las unidades de distribución, tales como robos a las unidades de distribución o peor.
* Modo Escritura: Si un actor no autorizado accede al dato en cuestión en modo escritura podría comprometer la integridad de los datos, problemática conocida como Tampering, o suplantar la identidad de una o más unidades de distribución, problemática también conocida como Spoofing.

1. Identifique cuatro vulnerabilidades del mismo 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
   1. Un ataque DDoS (Denial of Service) sobre el servidor de que maneja el estado de distribución de paquetes impediría a la empresa conocer el estado de los vehículos y la entrega de paquetes realizada, exponiendo a los vehículos a riesgos de seguridad.
   2. Un ataque DDoS sobre el servidor de manejador de ordenes impediría a la empresa prestar el servicio a nuevos clientes calcular nuevas rutas para los vehículos por lo que la empresa no podría operar.
   3. Una falla crítica como un desastre natural sobre los servidores de distribución de paquetes y el servidor de órdenes de recogida sería fatal para la empresa, ya que estos no cuentan con redundancia para distribuir la carga de trabajo, no se podrían agregar nuevos paquetes y se perdería la vigencia en el estado de los vehículos.
   4. Ya que la comunicación que se da entre los servidores de manejador de órdenes y el de distribución de paquetes se da por medio de la plataforma de integración, un acceso no autorizado que lea los mensajes que se dan por medio de la plataforma, si estos no están encriptados por la plataforma podría vulnerar la privacidad de los clientes y de todo el sistema, facilitando robos.
2. Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución. 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). Además, debe justificar los mecanismos propuestos. Es decir, identifique explícitamente qué vulnerabilidad resuelve y justifique.
   1. Y 3.2. Un firewall no es suficiente para detener un ataque DDoS ya que este bloquearía los puertos indiscriminadamente evitando así que entren los paquetes legítimos por lo que la empresa podría implementar hardware de análisis de paquetes previo a la conexión de red a los servidores que filtre los paquetes de ataque antes de que alcancen los servidores y de esta forma evita congestionar la banda ancha permitiendo un servicio adecuado a sus clientes, este hardware podría ser implementado antes de la plataforma de integración y de esta forma protegería a todos los servidores del sistema.
   2. .
   3. Para una falla crítica sobre los servidores de órdenes de recogida y ordenes de recogida se pueden implementar servidores de respaldo en locaciones remota que se encuentren en modo “Pasivo” y reciban un “HeartBeat” de los servidores principales de manera periódica, en caso de que estos dejen de recibir el latido por un periodo anormal de tiempo, el tráfico es redirigido a estos por medio de la plataforma integrada y de esta forma se evita perder disponibilidad en la prestación del servicio o información vigente del estado de los vehículos.
   4. La plataforma de integración puede implementar un protocolo de encriptación entre sus puntos de entrada que proteja la confidencialidad de la información. Para esto, al conectarse un nuevo punto de entrada a la red de la plataforma, esta le puede pedir un certificado para comprobar su legitimidad por medio del protocolo asincrónico RSA, una vez verificada, se puede utilizar las llaves publicas ya compartidas para compartir una llave sincrónica que use un protocolo AES 128 que comparten los puntos de acceso y se cambia periódicamente de manera semi-aleatoria, una vez confirmada la llave sincrónica el nuevo punto de entrada se puede comunicar con el servicio que necesite por medio de la plataforma.