Análisis y entendimiento del problema

1. La compañía de Colpensiones presenta una arquitectura de sistema que incluye 3 servidores encargados de un área operacional de la empresa. El primero, supone un portal web para que los afiliados tengan la oportunidad de consultar su información en línea y su estado de cuenta. Dicho servidor es ejecutado en la oficina principal la cual contiene una copia de seguridad tanto de memoria y procesamiento. Dicho servidor es uno de los mas críticos, ya que maneja toda la información monetaria y personal de los diferentes clientes. Dicho servidor contiene información confidencial, la cual contempla los documentos de cada afiliado, sus respectivas contraseñas, y el valor monetario de cada afiliado. Dichos datos tienen que estar totalmente confidenciales ya que permiten identificar los ingresos de cada uno de los afiliados. Si por alguna razón, se llega a ejecutar un ataque cibernético, este afectaría gravemente el funcionamiento de la empresa; teniendo acceso a los datos mediante la escritura y lectura podría robar o usurpar los valores de las pensiones de cada afiliado, incrementando sus ingresos o eliminándolos del sistema. Se podría presentar un (Man in the middle) haciéndose pasar por algún usuario, solicitando y modificando la información de los usuarios. Por otro lado, los computadores de la empresa están conectados a una subred en la que corre el servidor de la web. Eso es un factor de riesgo muy grande, ya que no solo con tener acceso al protocolo del servidor, se tiene acceso a la información de los afiliados, si no de la empresa. El firewall puede evitar malwares y viruses pero no puede evitar el problema del man in the middle.
2. Se pudieron evidenciar diferentes vulnerabilidades en el sistema, para ello toca evaluar cada una de las mismas en torno a la confidencialidad, integridad, autenticación y repudio de los datos. La primera vulnerabilidad y la mas critica es en cuanto al “Man in the middle” y ocurre cuando un atacante intercepta y se modifica la información de Colpensiones haciéndose pasar por un afiliado y/o empleado cuando realmente es una identificación falsa. Esta vulnerabilidad afecta la autenticación de la información, en términos de procesamiento de la información, dicho atacante puede ocupar y anular los servidores de diferentes maneras, enviando y sobrecargando los procesos para que el servidor se ejecute mucho más lento. Dicho procesamiento de la información también puede ocupar la memoria de la empresa, generando un ataque de denegación del servicio. Otro problema que se puede presentar es el de la confidencialidad, ya que, si no se cifra la información importante y se envía en texto plano, cualquier atacante podría obtenerla y atacar a Colpensiones como se había mencionado anteriormente. Por otro lado, la integridad es otro factor que se podría ver afectado, ya que si algún atacante reescribe la información y la envía sin poder identificar su origen si es de un afiliado o un atacante. Por último, el repudio es uno de los factores que más se verían afectados, ya que un atacante puede modificar la información de los diferentes afiliados y el servidor no puede negar que recibió dicha modificación por lo que tendrían que asumir dichas modificaciones ya que no pueden determinar la autenticidad del emisor. Es decir, si se modifica una cuenta, el receptor no puede negar que recibió la modificación y el mensaje incluso si no se tiene la autenticidad del emisor, por lo que no se puede determinar si fue una modificación realizada por atacante o afiliado.