Integrantes: Julián Esteban Osorio Ramírez y Louis Fernando Gualtero

Códigos: 201714171 y 201728201

A. Análisis y entendimiento del problema
    a. Identificar los datos que maneja el portal web y que deben ser protegidos: (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 afectarla entidad?)

    La información más importante que maneja la empresa tiene que ver con las personas (afiliados) porque se maneja la historia laboral de los afiliados. También la información de las empresas (aportantes) ya que se guarda información de pago, y deudas de todas las empresas colombianas, que tienen que pagar la pensión de sus trabajadores a través de empresas especializadas. Por último, hay información de empleados independientes los cuales tienen doble papel de afiliados y aportantes. Esta información es altamente sensible, entonces hay altos riesgos de corrupción. Es un recurso crítico y debe estar protegida, no sólo contra inconsistencias sino también contra posibles fugas o modificaciones indebidas. En un futuro cada estación de trabajo será virtualizada y accederá al proceso BPM (procedimiento almacenado) que le sea permitido, esto haría que el manejo de datos en la base de datos sea mas seguro por un filtro extra de seguridad en el VMM.
    La modificación de datos por un actor no autorizado puede afectar la credibilidad de la empresa y su capacidad de operar efectivamente. En caso de que se cambie un dato en la base de datos la capacidad perdería la capacidad de llevar un récord preciso para cada uno de sus clientes.

    b. Identifique cuatro vulnerabilidades de este sistema, teniendo en cuenta únicamente aspectos técnicos 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.

    Teniendo en cuenta que es una empresa con altos riesgos de corrupción por el tipo de información y recursos que maneja, esta se encuentra expuesta a diferentes tipos de exposición de datos sensibles. Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

    -Una de las principales vulnerabilidades es la de poder acceder a la información de los afiliados y modificarlos, si un atacante utiliza el método de ataque de man-in-the-middle. Afectando la integridad de los datos. Esto se puede presentar si no se realiza un correcto cifrado de los datos, autenticación y autorización.

    -Si una persona no tiene los permisos adecuados para ver, eliminar, agregar información de los afiliados y/o aportantes; se puede presentar un problema de elevación de privilegios si no se tiene un buen manejo de la autorización de los usuarios a ciertas funciones.

-En el caso en el que un atacante acceda a los datos de los afiliados y aportantes. Estos datos pueden ser utilizados para realizar actos de fraude y demás; intentando establecer comunicaciones con otras empresas u otros afiliados de la misma empresa o con empresas aportantes. Para obtener datos confidenciales los cuales no le serían permitido sin información de un miembro de la empresa.

-Los datos de las B.D pueden verse afectados por un ataque de ransomware, en donde se le pida a colpensiones pagar una cuantiosa suma para volver a obtener el acceso a sus datos. Esto se podría presentar si no se prueba la autenticación de todos los usuarios, se tiene un método de cifrado bastante débil o no se tiene.