1. **[20%] Análisis y Entendimiento del Problema. En el sistema descrito en el párrafo anterior:**
2. Identifique los datos que deben ser protegidos por la aplicación Novasoft financiero en línea. Justifique su respuesta (para cada dato responda la pregunta ¿Si un actor no autorizado consigue acceso al dato mencionado, ¿cómo podría afectar la empresa?

* Credenciales de cada usuario:

Es de vital importancia proteger las credenciales de los usuarios, al ser un sistema financiero si un actor no autorizado consigue acceso a las credenciales además de conocer datos sensibles del usuario también podrá realizar transacciones lo que genera una pérdida de confiabilidad y de usuarios a la empresa.

* Transacciones realizadas por cada usuario:

Al manejar un historial transaccional de los usuarios es importante proteger el mismo, ya que si esta información es adquirida por un actor no autorizado podría poner en riesgo la seguridad del usuario y una fuerte violación a su privacidad, que conlleva problemas legales para la empresa además de perdida de la confiabilidad y probablemente la perdida de usuarios.

* Malware:

Al estar trabajando sobre una plataforma financiera en línea es importante tener en cuenta que si un actor no autorizado logra instalar malware en el sistema puede generar problemas para la compañía como:

* + Saturación de peticiones o de red: algunos tipos de malware son instalados con el objetivo de generar un ataque DOS, lo que pone en riesgo que la plataforma deje de funcionar por una cantidad de tráfico simultaneo no soportada.
  + Daño de datos: otro tipo de malware consiste en destruir los datos de un sistema, lo que representaría grandes pérdidas y problemas legales a esta plataforma financiera.

Finalmente es importante hacer un análisis acerca de la naturaleza de la empresa, al ser un sistema financiero cualquiera de los problemas anteriormente mencionados es catastróficos para la compañía, al estar tratando de datos financiero y manejar dinero y deudas de por medio los daños económicos y legales serían irreparables para la compañía.

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

* No hay forma de controlar el número de peticiones que es enviada por un cliente al servidor, lo que permitiría que se realizara un ataque de denegación de servicios mediante la saturación del servidor.
* Puede haber contraseñas débiles lo que permitiría que mediante algún método de cálculo masivo de contraseñas o un ataque de diccionario obtener la contraseña de algún usuario. Elevación de privilegios.
* Los algoritmos de cifrado usados son ampliamente conocidos en la industria por lo que podrían ser reversados. Si las llaves son descifrables entonces podría haber un ataque man in the middle.
* No existe ningún tipo de protección en contra de malwares previamente mencionados lo que permitiría una posible pérdida/alteración/daño de datos, y al ser amplio el número de malwares existentes las consecuencias son incalculables.

1. **[10%] Propuesta de Soluciones. Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución/mitigación. Justifique brevemente por qué el mecanismo propuesto resuelve la vulnerabilidad.**

* Para solucionar la vulnerabilidad del número de peticiones enviadas es necesario desarrollar un mecanismo que permita establecer un número máximo de peticiones enviadas por un cliente, ya sea mediante una dirección ip en el caso de comunicación mediante protocolo HTTP/TCP, mediante un identificador de usuario o identificador de sesión. Esto con la intención de evitar un ataque DOS. Algunos de estos mecanismos son:
  + Configuración de Routers y Firewalls para detectar ip’s invalidas.
  + Manejo de logs con toda la actividad de los clientes.
  + Uso de IDS/IPS **(intrusion detection/prevention system)**
* Para solucionar la vulnerabilidad en las contraseñas se puede principalmente sugerir una mejor asignación de contraseña por parte del usuario, de igual manera se puede implementar requerimientos de contraseña, es decir, no permitir al usuario establecer una contraseña que no cumpla con ciertas especificaciones.

También se puede mitigar esta vulnerabilidad mediante la utilización de certificados para validar la identidad del usuario.

* Para la vulnerabilidad del uso de algoritmos ampliamente conocidos en la industria se puede mitigar mediante el uso de algoritmos de cifrados simétricos y asimétricos menos conocidos como:
  + Simétrico:
    - TDES
    - RC2
    - ICE
    - IDEA
    - GOST
    - AES
    - Rindjael
    - Serpent
    - Blowfish
    - Twofish
  + Asimétrico
    - RSA
    - DSA
    - ElGamal

Otras estrategias para mitigar esta vulnerabilidad son:

* + Uso de Salt para dificultar el descifrado por parte de un actor no deseado.
  + Uso de ambos cifrados: simétrico y asimétrico.
  + Uso de dos o más algoritmos de cifrado.
  + Uso de certificados para cifrar y agregar dificultad para el descifrado por parte de un actor no deseado.
* Para mitigar la vulnerabilidad a obtener malware en el servidor es necesario tener en cuenta las siguientes acciones:
  + Detectar: cualquier irregularidad en su servidor o en la actividad de algún cliente puede ser sinónimo de un malware.
  + Eliminar: es primordial detener el servidos en el instante que se detecte un malware, para así encontrar el gusano y eliminarlo. También se recomienda la adquisición de software para la detección y eliminación de Malware.
  + Prevenir: es necesario mantener actualizado los parches y los servicios de terceros. También se recomienda la adquisición de software de protección contra malwares y tener una buena política de asignación de contraseñas (remítase al apartado número 2 de este punto).

Como recomendación adicional debe considerarse la contratación de una empresa que se encargue de la auditoria del sistema en cuanto a Malwares.

Como consideración extra se recomienda la contratación de una empresa especializada en seguridad informática para realizar tareas de prevención, auditoria, detección y eliminación de amenazas.

Referencias:

-https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/