**Caso de Estudio 2**

**Ingeniería de Sistemas y Computación**

**ISIS 2203 Infraestructura Computacional**

**Canales Seguros Logística y Seguridad Aeroportuaria**

1. **[20%] Análisis y Entendimiento del Problema.**
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?**
   1. **Instalación de Malware**

Si aparece un actor no deseado, podría instalar programas maliciosos que podrían provocar daños importantes en el sistema. En caso de que sea un malware, se podrían tener varias consecuencias. La intrusión de un gusano en el sistema puede provocar un gran tráfico en el sistema o en la red y pueden ser saturados, ya que el objetivo de un gusano es replicarse al máximo. Dado que estamos hablando del servidor que administra las transacciones financieras, esto representaría grandes pérdidas para la empresa. También, en el caso de que los gusanos tengan un *payload*, se podrían dañar los datos del sistema, de la computadora o de la red. Además, si estos *payload* instalan una puerta trasera, es probable que traigan otro malware para que controle la computadora. Como resultado, los sistemas de la empresa colapsarían, lo que afectaría los datos de transacción, las facturas y el funcionamiento de los sistemas de la oficina central directamente. En consecuencia, se formaría un desastre financiero para la empresa, desde servidores de saturación hasta la destrucción del sistema. Adicionalmente, este problema causaría una disminución y afectación en la imagen de la compañía y, por lo tanto, una disminución en la asistencia a su servicio.

* 1. **Modificación de datos**

Si un actor externo modifica los datos presentes en la aplicación en línea de Novasoft financiero se podría convertir en un gran problema y generar situaciones complicadas para la compañía. Por ejemplo, al eliminar las cuentas de los clientes que tendrían una gran deuda con la empresa, se podría generar una pérdida financiera. Adicionalmente, esta situación puede generar inconvenientes y situaciones tensas entre el cliente y la empresa, y deteriorar la imagen de la empresa. La imagen de una compañía es primordial, especialmente en el ámbito de la seguridad, y si esta se deteriora se tendría como resultado una disminución de clientes y una pérdida de dinero. También, los actores externos que tengan acceso a los datos pueden hacer modificaciones a la información a su conveniencia que ponen en riesgo la integridad de estos.

* 1. **Robo de datos**

Un actor no deseado podría robar datos confidenciales de la compañía que pondrían en duda la seguridad del sistema de la compañía y utilizar dicha información para hacer cualquier tipo de acto ilegal. Por ejemplo, un usuario común del sistema puede ser redirigido a un servidor fraudulento y, cuando deba identificarse con su nombre de usuario y contraseña, será robado por la persona con acceso directo al servidor fraudulento. El ladrón tendrá acceso a todos los datos existentes, y ningún otro dato del sistema será confidencial. Informes, bases de datos, estados financieros, datos bancarios, transacciones, entre otros. Como resultado, el actor podría vender los datos a los competidores, o simplemente exponerlos sin la certeza de que los datos se utilizarán indebidamente o no.

* 1. **Usurpación de identidad (Spoofing)**

Si el actor por los métodos anteriores logra robar la contraseña y tener acceso al sistema como un empleado, entonces puede tomar la identidad de éste y luego reclamar ser ese empleado y falsificar información diversa sobre él. Además, el actor maligno no solo tendría información del empleado a el cual está suplantando sino también a información de otros empleados, directivos y clientes dependiendo los permisos autorización que tenga el empleado que fue suplantado. Esto podría causar un verdadero problema dentro de la empresa, especialmente si la persona en cuestión es una persona con responsabilidades importantes. Todos estos problemas que causa la suplantación de identidad deben ser prevenidos y manejados por el mismo sistema para que se compruebe que la persona que está ejerciendo dichas acciones realmente es el individuo verdadero y no un actor externo suplantándolo. En resumen, las vulnerabilidades que tenga un sistema que faciliten la suplantación por agentes externos puede ser caótica dentro de un sistema financiero en línea como el de Novasoft. Ya que, constantemente se están realizando registros de transacciones y se está manejando información muy importante, y por lo tanto es de suma importancia que el sistema prevenga y maneje este tipo de vulnerabilidades.

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.**
   1. **Almacenar información confidencial sin cifrar (Criptografía)**

Se relaciona con muchos puntos vistos anteriormente. Esta vulnerabilidad es bastante peligrosa, pues durante los ataques, si la información no se encuentra encriptada, esta misma sería fácil de robar o sobrescribir. Lo cual, mediante la encriptación podríamos evitar o al menos dificultar. Por lo anterior, la información y en especial los datos de alta importancia para la empresa, como las cuentas, debe ser encriptada para evitar que esta sea robada o modificada por terceros sin autorización.

* 1. **Buffer Overflow (Desbordamiento de búfer)**

El Buffer Overflow es un error de computadora y también puede ser provocado y explotado intencionalmente para violar la política de seguridad de un sistema. Si, en uno de los servidores, podemos sobrecargar el búfer con más recursos de los que puede admitir (principio del *Buffer Overflow*), un usuario puede generar un error en el programa y tener acceso a la pila y así tomar el control del sistema.

En el servidor 3 (página web), el atacante podría usar este servidor, y cuando se encuentra en un campo se le solicita que ingrese un nombre de usuario para ver, por ejemplo, ciertos documentos de experiencia que requieren una conexión. El atacante inundaría el número de caracteres (mucho más alto que el número asignado originalmente) para luego acceder a la pila de instrucciones y lanzar las instrucciones que deseen. Podría modificar el código y lanzar un shell líder al sistema y tomar el control de la página web.

Podemos imaginar este mismo proceso en los otros servidores, al igual que para los correos, con riesgos que pueden ser aún mayores si logran llegar al servidor 1 que administra el sistema financiero.

* 1. **Autenticación débil**

Un clásico a nivel de seguridad de la plataforma informática. Dado que la mayoría de los usuarios solo tienen que iniciar sesión con una contraseña y un inicio de sesión para acceder al sistema, por ejemplo, para la administración del sitio web, pero también para el correo o "Sistema Time and Attendance", si los usuarios y la plataforma permiten contraseñas simples, el atacante puede forzar su acceso al sistema. Esto sería aún más serio si afecta al personal del sistema financiero, operando tan simplemente como con las contraseñas. El atacante solo tendrá que encontrar la combinación correcta para ingresar al sistema y darse cuenta de lo que se ha dicho en el punto 1, por ejemplo. Para encontrarlos puede usar algunas herramientas como "John the Ripper" para "descifrar" la contraseña. Por supuesto, una contraseña con menos caracteres, siendo solo una combinación alfanumérica, o siendo palabras existentes generalmente es más fácil de encontrar y, por lo tanto, más rápido para que el atacante ingrese al sistema con el fin de robarlo. información.

* 1. **Configuración de seguridad incorrecta (Security Misconconfiguration)**

Una mala configuración de seguridad puede llevar a consecuencias bastante altas dependiendo de las vulnerabilidades. Esto conlleva a que personas puedan acceder a información a la cual en principio no deberían tener acceso. Por ejemplo, una configuración errónea podría resultar en la creación de una cuenta anónima dentro del servidor de Time and Attendance porque es una estructura diseñada para que un empleado cree una cuenta y la use. Esto permitiría un fácil acceso a la información presente en el sistema que habría sido mal configurada. Estas cuentas anónimas también podrían usar una de las vulnerabilidades vistas anteriormente: el Desbordamiento de Buffer. Lo que paralizaría una buena parte del servidor.

Por ejemplo, para el sitio web, esto puede dar acceso a los comentarios dejados por el programador y, por lo tanto, proporcionar información que pueda ser sensible al correcto funcionamiento del sitio web en el servidor 3. El atacante podría usar esta información para encontrar las fallas que permiten poner sus manos en el sitio web, y así tener control de él que resulte en las consecuencias observadas anteriormente, y puede dañar la reputación de la empresa. Los errores de configuración son muchos y variados, y una cuenta anónima podría, por ejemplo, cambiar los derechos y la política de seguridad de los servidores, hasta llegar a las cuentas financieras del servidor 1, permitiendo, por ejemplo, la vulnerabilidad "c" vista justo antes. y así introducir este servidor, y obtener información confidencial.

1. **[10%] Propuesta de Soluciones.**
2. **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. En sus justificaciones tenga en cuenta aspectos relacionados con eficacia, costo, eficiencia, flexibilidad, aspectos de implementación, y otros aspectos técnicos que considere convenientes.**
   1. **Instalación de Malware**

Esta amenaza es una de las más peligrosas, ya que primero debe detectar este virus o gusano, el cual se puede propagar en varias máquinas. Para hacer esto, uno debe comenzar instalando antivirus y firewalls. Acompañado por más de un software antimalware para bloquear todo software considerado como malicioso. Sin duda, esto será más costoso que un simple antivirus, pero permitirá una mejor detección de virus y, por lo tanto, podrá actuar más rápidamente durante un ataque. Además, es necesario actualizarlos regularmente para que el sistema este mas actualizado frente a las posibles amenazas. Los gusanos, a su vez, pueden mitigarse manteniendo el sistema actualizado, solicitando que se cambie la clave después de unos días y manteniendo la información cifrada, así como las mismas recomendaciones que se deben seguir al manejar los virus. Además de usar un antivirus lo más importante es reaccionar rápidamente para evitar la propagación de estos programas maliciosos.

* 1. **Modificación de datos**

Con respecto a la modificación de los datos, esto pasa antes por los derechos de los usuarios sobre los archivos. De hecho, dar acceso de escritura a los usuarios sin ninguna razón para modificar el archivo supone un riesgo adicional. Lo mejor sería mantener una revisión constante y exhaustiva del código fuente para descubrir estos agujeros en el código y hacerlo por alguien que no sea el programador. Otra alternativa sería realizar copias de seguridad periódicas de los datos, esto requiere más espacio de almacenamiento, pero permitirá comparar algunos datos e inconsistencias si ha habido cambios.

De igual forma, una solución más barata, sería un certificado digital para asegurarse de que está en el servidor correcto o en el sitio correcto, y por lo tanto no debe enfrentar un servidor falso que luego recupere los datos como Contraseña de la persona en esta trampa.

* 1. **Robo de datos**

Respecto al robo de información, cuando es robada, puede ser difícil detectar al atacante. Como resultado, las soluciones a esto son soluciones para evitar el robo, por lo que hablamos más sobre la prevención.

Para reducir el riesgo de robo, la información debe estar encriptada. Pueden estar con una clave simétrica para tener un tiempo que cuesta menos que las claves asimétricas. Esta clave solo es conocida por algunos empleados para proteger datos confidenciales. Estas claves se almacenarían asimétricamente con una clave pública para cada persona con la clave simétrica. De esta forma, solo se puede descifrar mediante una clave privada que posee el propietario.

Además, para evitar el espionaje industrial, también es posible con un poco más de costo instalar antispyware para detectar spyware.

* 1. **Usurpación de identidad (Spoofing)**

Para evitar el robo de identidad, inicialmente es necesario que las contraseñas tengan un nivel suficientemente alto de seguridad. Una buena contraseña requiere un número mínimo de caracteres, con una combinación de letras (minúsculas y mayúsculas), números y caracteres especiales, que preferiblemente no conformen una palabra real. Una buena idea es tomar una oración y guardar las iniciales. También es obvio no almacenar esta información a la vista en el sistema y protegerla como se vio anteriormente.

Además, para autenticar la conexión a uno de los sistemas, el usuario debe usar un certificado de autenticación para probar su identidad.

También podríamos limitar el número de intentos de acceso, por lo que la cuenta se bloquearía después de un cierto número de intentos. Y así, para las comunicaciones entre empleados, sería posible utilizar una firma electrónica.

Y, de manera más general, además del software que se debe instalar. Adicionalmente se debería brindar capacitación a los empleados acerca del buen manejo de datos y creación de contraseñas, pues un factor importante en las vulnerabilidades es causado por el factor humano. Estos pequeños detalles pueden hacer una gran diferencia.