Caso 2

Infraestructura computacional

Nicolás Gómez - 201426109
Christian Potdevin - 201424177

A. Análisis y Entendimiento del Problema.

1) Amenazas

i) Una amenaza para la aplicación Novasoft Financiero online es la caída del servicio, que podría darse de muchas maneras. En primer lugar, podrían ocurrir desastres naturales, como un terremoto, una inundación, o cualquier otro fenómeno que pueda llegar a afectar el servidor que está soportando la aplicación. Otra posibilidad es que se diera una emergencia ambiental, como un corte de la energía, pero esta amenaza es mucho más fácil de mitigar, ya que se pueden tomar medidas preventivas para este tipo de situaciones. Finalmente, es posible que llegue software malicioso al servidor. Esto podría pasar por una persona que llega hasta el servidor en físico e inserta el software mediante una USB. En caso que cualquiera de estas cosas llegara a suceder, se detendría completamente el funcionamiento de la aplicación, y nadie podría acceder a la información que ésta tiene. Esto podría ser catastrófico para Logística y Seguridad Aeroportuaria S.A ya que si el servidor no está habilitado no se podrían llevar a cabo transacciones con él. Esto afectaría la disponibilidad del sistema.

ii) Ya que existen varias oficinas que están en constante comunicación con el servidor de la aplicación, es posible que se de espionaje en los medios de transmisión. Si alguien conoce los canales de comunicación de Logística y Seguridad aeroportuaria S.A, puede que esta persona sea capaz de interceptar los mensajes que Novasoft Financiero online envía o recibe. Esto puede no ser crítico para la empresa, ya que se sabe que los mensajes están encriptados, pero no se sabe que métodos de encriptación se usan, por lo cual puede que sea fácil para la persona que intercepta los mensajes descifrarlos. Esto afectaría la confidencialidad e integridad que tiene el sistema.

iii) Dado que no se tiene información sobre cómo se guarda la información en los servidores de Novasoft, se puede decir que esto es una amenaza, ya que es información sensible a la cual solo las personas autorizadas deberían tener acceso. En caso que una persona lograra acceder directamente a la base de datos del servidor podría extraer toda la información, lo cual no sería bueno para Logística y Seguridad aeroportuaria S.A porque puede que la información financiera de la empresa llegue

hasta algún competidor o alguien que pueda aprovecharse de esto. Esto afectaría la confidencialidad e integridad del sistema.

iv) Si los usuarios que piden información al servidor de Novasoft no están haciendo una autenticación adecuada, puede que se de suplantación, donde alguien se hace pasar por Novasoft. Para que esto pasara la persona tendría que conocer los métodos de cifrado que se están utilizando, lo cual podría ser fácil si estos son sencillos. Si esto sucediera podría ser catastrófico para la empresa ya que recibir información falsa sobre el estado financiero de la empresa podría llevar a tomar decisiones que no serán las adecuadas.

v) De igual manera que en el anterior literal, podría darse que los usuarios usen claves débiles y haya suplantación en el otro sentido, donde alguien se hace pasar por una persona con acceso a más información. Como se mencionó antes, no es deseable que terceros tengan acceso a la información del estado financiero de la empresa.

2) Vulnerabilidades

i) Como el sistema time & attendance está ubicado en el mismo servidor que maneja el correo electrónico entonces se podría acceder a este a través del sistema de correos.

ii) Los servidores de Novasoft cuentan con su propia base de datos, y dado que estas máquinas no tienen memoria ilimitada, puede que se llene y se empiece a perder información.

iii) Adicionalmente, Novasoft está en el límite de usuarios potenciales/usuarios concurrentes. En caso que la compañía se expanda un poco, el desempeño de la aplicación se verá gravemente afectado.

iv) Como se mencionó anteriormente, los usuarios con acceso a los archivos de Novasoft, de la aplicación de correo electrónico, o de Time and Attendance podrían escoger claves débiles que sean fáciles de hallar mediante un ataque de fuerza bruta, lo cual comprometería la información de la empresa.

v) Tanto el servidor de correo electrónico como las aplicaciones financieras Novasoft y OpenERP mantienen información importante que no debería salir de la compañía, por lo cual es necesario encriptar la información no solo al momento de enviarla sino también al momento de almacenarla en el servidor.

B. Propuesta de Soluciones.

i) El servidor de la aplicación debería estar en un lugar seguro donde se pueda prevenir el acceso de personas sin autorización. Adicionalmente, debería ser un lugar con las capacidades de mantener el servidor corriendo a pesar de fallas ambientales, es decir, el lugar debe tener plantas de energía y la ventilación adecuada. Finalmente, puede que un desastre inevitable ocurra, por lo cual el servidor debería un tener un backup.

ii) Se debe utilizar cifrado asimétrico para el intercambio de información entre la aplicación y los usuarios, y la llave privada de cada quien debe estar guardada muy bien para que nadie tenga acceso a ella. De esta manera, así alguien sea capaz de interceptar los mensajes, se sabe que es muy poco probable que sea capaz de descifrarlos.

iii) La información que se almacena en el servidor de la aplicación también debería ser encriptada. En este caso, cifrado simétrico sería suficiente, donde se tiene una llave que encripta y desencripta la información. En caso que se implementara esta solución también habría que considerar dónde y cómo se almacenará la llave, ya que si se guarda sin seguridad extra sería lo mismo que no haber hecho nada. Para esto, debería implementarse un mecanismo donde la llave es encriptada con el hash de una clave secreta, y solo quien se sepa la clave secreta podrá desencriptar la llave.

iv) Si se utilizara cifrado asimétrico, podría verificarse la identidad del servidor mediante el uso de las llaves privadas. En caso que no se quiera cambiar el método de cifrado, podría adjuntarse también el certificado digital del servidor en cada mensaje, y de esta manera los usuarios tendrán la certeza que cuando reciben un mensaje éste proviene del servidor.

v) El administrador del sistema debería encargarse de implementar políticas de seguridad para evitar este tipo de amenazas. Si se implementara un mecanismo que obligue a los usuarios a tener al menos una mayúscula y un número en su clave, esto disminuiría las probabilidades que alguien descubra la cuenta de un usuario y acceda a la información, ya que no podrá realizar ataques de fuerza bruta.