CASO 2

INFRAESTRUCTURA COMPUTACIONAL

JUAN FELIPE RAMOS 201616932  
SERGIO CÁRDENAS 201613444  
MARIA ALEJANDRA ABRIL 201530720

1. Análisis y entendimiento del problema
2. Abarcando las funcionalidades del servicio Novasoft Financiero en Línea podemos analizar que datos deben ser protegidos y porqué:

Inicialmente, los datos financieros son de vital importancia para la compañía, por lo cual su protección (al menos su no alteración) debe ser garantizada. De no ser protegidos, valores contables como valores de nómina dentro de “Logística y Seguridad Aeroportuaria S.A” podrían verse alterados, generando, por ejemplo, errores en pagos de nómina de los diferentes clientes del servicio de Novasoft Financiero en línea e incluso generando errores en contratos de adquisición de los servicios de transportistas o problemas legales por el cálculo erróneo de la deducción de impuestos.

De igual manera, es esencial proteger la información que acredita a los usuarios de Novasoft Financiero dentro del sistema; esto incluye su login, password y rol, además de la información del usuario para garantizar el correcto funcionamiento del sistema (como nombre y empresas con las cual se relaciona dentro del sistema), esto con el fin de impedir acceso a información no pertinente que pueda ser, en el peor de los casos, modificada, generando un funcionamiento erróneo del sistema Novasoft Financiero.

1. Se pueden identificar las siguientes vulnerabilidades dentro del sistema de Novasoft:
2. Aunque se realice una autenticación a nivel de sistema operativo, bien las contraseñas pueden ser débiles y no son prenda de garantía para autenticar un usuario. Esto hace el sistema frágil ante un ataque de fuerza bruta en el que se intentan probar todas las configuraciones de autenticación (login y password) a fin de ingresar al sistema. Así, la información financiera de los clientes está parcialmente expuesta.
3. Los datos que se transmiten desde el servidor de Novasoft Financiero no están explícitamente cifrados, lo cual los hace vulnerables a cualquier atacante que decida escuchar la transmisión. Dado que la información que se intercambia por medio de este canal puede ser sensible para el cliente del servicio, por ejemplo, información respecto a contratos celebrados entre clientes del sistema, el compartir esta información puede ser un gran riesgo.
4. A lo largo de la transmisión de los datos no hay un mecanismo que garantice que los datos no se han visto alterados, ya sea por motivo de errores en la red o por un intento de ataque. De esta manera pueden obtenerse resultados que, aunque lógicos, son equivocados y afectan, al ser información financiera la que se transmite, el funcionamiento de cualquier cliente de Novasoft Financiero. Por ejemplo, puede haber errores en los valores de contabilidad o cálculo de impuestos lo que redunda en problemas fiscales.
5. No se tiene control sobre el número de peticiones que se realizan, razón por la cual el sistema es vulnerable a ataques como DoS (Denial of Service) o DDoS (Distributed Denial of Service) que consisten en la inutilización de un servicio dado por Novasoft mediante el llamado excesivo al mismo (hasta el desbordamiento).
6. Propuesta de soluciones
7. Una posibilidad de garantizar la autenticación es utilizar certificados para avalar identidades. De esta forma, hay un mayor costo en términos de tiempo debido a que se generan los certificados correspondientes para avalar las identidades tanto del cliente como del servidor. Sin embargo, es necesario con tal de proteger la información dentro de Novasoft Financiero.
8. Con el fin de proteger la información de posibles ataques es necesario cifrarla. Por tanto, una posible propuesta consiste en, buscando disminuir la complejidad, enviar mediante cifrado asimétrico las llaves de un algoritmo de cifrado simétrico para así establecer la comunicación de una forma segura. De esta manera, si el contenido a cifrar es corto (del tamaño de la llave simétrica) la complejidad del algoritmo asimétrico se reduce, lo cual es significativamente mejor a cifrar todo usando un algoritmo de cifrado asimétrico y es lo suficientemente seguro al cifrar las llaves de cifrado simétrico (que es necesario para establecer el enlace).
9. Para verificar que no hubo cambios en a lo largo de la transmisión se puede realizar la verificación con un digest de la información que se envía. De esa manera, se calcula el hash de la información que se envía y el receptor se encarga de recalcular para confirmar si existen diferencias entre el hash calculado y el hash recibido del emisor. Si estos resultados difieren entonces hubo alteración de la información enviada durante la comunicación.
10. Como solución a los eventuales ataques DoS, se pueden contratar empresas que se encargan de que este tipo de ataques se reduzcan sustancialmente. Las ventajas que incluyen este tipo de servicios es dar la posibilidad de tener acceso a personal capacitado para monitorear el uso de los servicios dados por Novasoft. Por otro lado, también es conveniente poseer algún tipo de control de peticiones propio en donde la cantidad del uso de los servicios brindados puede ser monitoreada. De esta manera, se puede reconocer que elementos pueden estar siendo víctimas de un ataque.

**Bibliografía**

* Sean Leach, VP of Technology, Verisign, special to Network World. (2013, September 17). Four ways to defend against DDoS attacks. Retrieved October 26, 2017, from https://www.networkworld.com/article/2170051/security/ tech-primers-four-ways-to-defend-against-ddos-attacks.html