aCTIVIDADES FINALES

TEMA 7

Aarón Cañamero Mochales

25/02/2021

Índice:

[CONSOLIDACIÓN: 2](#_Toc65230058)

[APLICACIÓN: 5](#_Toc65230059)

CONSOLIDACIÓN:

1. ¿Qué diferencias existen entre un antivirus y una suite de seguridad?

Un antivirus es la medida de protección más conocida por los usuarios, este programa permite evitar infecciones por malware y sirve también para desinfectar equipos afectados y una suite de seguridad es la suma de varios programas de seguridad que son: antivirus, antispyware, antirootjit, antiphishing, antispam y contrafuegos, etc, etc.

1. ¿Qué es un centro de protección y respuesta ante amenazas?

Estos organismos estudian el estado de seguridad global de redes y ordenadores, dan servicios de respuesta ante incidentes a víctimas de ataques en la red, publican alertas relativas a amenazas y vulnerabilidades y ofrecen información que ayude a mejorar la seguridad de estos sistemas.

Están los servicios preventivos y reactivos.

**Preventivos**: Avisos de seguridad, búsqueda de vulnerabilidades, auditorías o evaluaciones de seguridad, configuración y mantenimiento to de herramientas de seguridad, aplicaciones e infraestructuras, desarrollo de herramientas de seguridad.

**Reactivos:** Gestión de incidentes de seguridad (análisis, respuesta, soporte y coordinación de incidentes de seguridad), Gestión de vulnerabilidades (análisis, respuesta y coordinación de vulnerabilidades detectadas).

1. Describe los dos tipos de políticas por defecto disponibles para los cortafuegos. ¿Qué ventajas e inconvenientes presenta cada una de ellas?

**Políticas permisivas**: Deniegan explícitamente el acceso a la red por parte de algunas aplicaciones, servicios, equipos o redes, permitiéndose el acceso al resto de aplicaciones.

**Políticas restrictivas:** Por defecto está prohibido el acceso a los recursos del sistema, debiendo autorizarse de forma explícita y caso a caso. Esta política es la más adecuada para la mayoría de ocasiones.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de trafico peligroso y sea permitido por omisión.

1. Enumera los tipos de cortafuegos que pueden encontrarse atendiendo a su ubicación en la red.

**Contrafuegos de equipo o de host:** Este cortafuego se instala en el equipo que se quiere proteger, analiza todo el tráfico que llega al equipo o sale de él y permite establecer qué aplicaciones puedan enviar y recibir información a través de la red.

**Cortafuegos de red o perimetrales:** Este cortafuego se ubica en un punto de entrado común a la red, como un router y actúa como barrera entre la red interna de nuestra casa u organización y la externa.

1. ¿Qué ventajas presenta un cortafuego de estado sobre uno de filtrado de paquetes? ¿Y uno de aplicación sobre uno de filtrado de paquetes?

El cortafuego de estado puede ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

El de aplicación permite detectar si un protocolo no deseado se filtró a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

1. ¿Por qué es importante mantener las aplicaciones actualizadas? ¿Y los plugins del navegador?

Es importante tener las aplicaciones actualizadas, para que los malware que puedan entrar en nuestro dispositivo no puedan hacer nada o que se les complique las cosas.

Con los plugins pasa lo mismo, podemos tener el ADBLOCK instalado en nuestro navegador, para que no entre software malicioso, pero este a la vez tiene que estar instalado.

1. ¿En qué se diferencia un CERT y un CSIRT? Cita tres ejemplos de cada uno de estos centros.

El CERT: Detención de Incidentes, Análisis de Logs y Análisis de Tráfico, Análisis forense, Intercambio automatización.

El CSIRT: Incidentes Gubernamentales, Estratégico de País, Políticas Gubernamentales.

1. ¿Qué es un software congelador? Indica las principales ventajas e inconvenientes de su uso.

Este Software especial de reboot and restore, cuando este se instala permite congelar el estado del equipo en un momento determinad, con la configuración y contenidos exactos que el equipo tenía en ese momento.

Se protege a los equipos frente a infecciones por software malicioso, ya que durante el procesa de restauración se elimina cualquier malware que haya infectado al equipo.

Como principal desventaja de su uso seria, cuando restauramos al mismo punto una y otra vez, las actualizaciones del sistema operativo y las distintas aplicaciones tampoco se guardan, por lo que el sistema quedará desactualizado al poco tiempo.

APLICACIÓN:

1. Un amigo se ha comprado un portátil que tiene instalado el cortafuego que trae por defecto el sistema operativo. ¿Qué consejos le darías a tu amigo para evitar infecciones por malware? ¿Y para evitar la pérdida de información en caso de que algún malware haya infectado el equipo?

Le diría a mí colega que se instalase un antivirus y que lo tenga actualizado y también que tenga actualizado todas las aplicaciones actualizadas.

También le diría que hiciese copias de seguridad, para poder tener todo más seguro.

1. Describe al menos cinco buenas prácticas que podemos seguir para minimizar riesgos de infección en nuestro dispositivo móvil.

Tener un buen antivirus para el ordenador instalada, tener las aplicaciones actualizadas correctamente, descargar las aplicaciones desde un sitio seguro, no abrir ningún correo que sea de posible fraude, usar contraseñas seguras.

1. Has recibido un mensaje de correo electrónico de un conocido dirigido a muchas personas, que forma parte de una cadena de mensajes y en el que se adjunta un archivo. Al observar el mensaje ves que ha sido reenviado anteriormente por muchas personas y que se te sugiere que lo reenvíes a tus conocidos. ¿Cómo deberías proceder para minimizar el riesgo de infección por malware en tu equipo? ¿Qué consejos podrías darle a tu amigo para contribuir a reducir riesgos de infección en correos electrónicos?

No mandaría ese correo a nadie ni tampoco descargaría nada, puede que en el archivo que viene adjunto haya algún tipo de malware que pueda infectar a nuestro equipo. Le aconsejaría que no abriese correo de SPAM, ni algunas que pueda pensar que sea fraudulento, le pondría un antivirus actualizado, le diría que protegiese más sus contraseñas de correo y pondré en su correo electrónico un programa de filtrado y bloqueo de correos sospechosos.

1. Has decidido instalar un software congelador en un cibercafé, pero no dispones de dinero para adquirir una versión comercial. ¿Existe algún programa que se adapte a tus necesidades? ¿Qué ventajas aporta la utilización de este tipo de producto?

Hay muchos tipos de Software congelador, que son gratuitos y si no se podría bajar la licencia de una manera ilegal. Las ventajas más evidentes son que cuando un usuario entre en el cibercafé y use un ordenador al cerrar sesión, aunque haya metido algún virus, esta para estar como nuevo sin nada, para el caso de que hayan metido algún virus.

1. Un cliente te dice que cree que su ordenador portátil “está infectado por un virus” porque le aparece una pantalla en la que le dice que la policía nacional ha detectado que ha hecho un uso fraudulento de ese equipo y que tiene que pagar una multa, cuando la realidad es que él no ha realizado ningún uso anómalo del mismo. También te comenta que no puede entrar en el sistema con normalidad, con lo que no puede guardar un trabajo en un dispositivo de almacenamiento externo. El cliente no dispone de ninguna otra copia de este trabajo, pero es muy importante recuperarlo.

¿Qué podrías hacer para solucionar esta incidencia?

Las soluciones más fáciles sería sacar el disco de almacenamiento y meterlo en otra máquina, para que pueda recuperar el trabajo y con el ordenador haría una restauración de fábrica, para eliminar el virus.

1. Después de solucionar el problema expuesto en la actividad anterior, intentas buscar el trabajo del cliente, pero descubres que el malware que ha infectado al equipo ha borrado muchos archivos de disco duro, entre ellos el trabajo. Decides utilizar una herramienta de recuperación de datos y consigues recuperar el trabajo. Indica qué consejos le darías al cliente para no volver a sufrir este tipo de situaciones.

¿Podrías recomendarle alguna herramienta que sea gratuita y fácil de utilizar?

Descargaría algún antivirus gratuito, con él va poder tener un equipo mucho más seguro, también le diría que tuviese más cuidado con los programas que se baja y donde se los baja, también le pondría un filtrado de correos de spam y sospechosos y por ultimo le descargaría es su navegador de preferencia un ADBLOCK en forma de pluggin para estar mucho más seguro.