Seguridad informática

Integridad, confidencialidad y disponibilidad

Entendemos por seguridad informática el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático (conjunto de hardware, software, personas y procedimientos) de integridad, confidencialidad y disponibilidad.

- Un sistema informático es íntegro cuando impide la modificación de la información a cualquier usuario que no haya sido autorizado con anterioridad.
- Un sistema informático es confidencial cuando impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.
- Un sistema informático es disponible cuando está en todo momento en funcionamiento y accesible para que los usuarios autorizados puedan hacer un uso adecuado de ellos.

Técnicas de seguridad activas y pasivas

Podemos diferenciar dos tipos de herramientas o prácticas recomendables relacionadas con la seguridad:

Las técnicas de **seguridad activa**, cuyo fin es evitar daños a los sistemas informáticos:

- El empleo de contraseñas adecuadas y seguras. Por eso es importante saber cómo elegir una contraseña segura y, si tenemos dudas, también podemos comprobar la seguridad de una contraseña. - La encriptación de los datos, que consiste en codificar la información con una contraseña, de tal manera que cualquier persona que la intercepte no pueda ver el mensaje original. Puedes probar a encriptar y desencriptar información online para ver como funciona.
- El uso de software de seguridad informática

Las técnicas o prácticas de **seguridad pasiva**, cuyo fin es minimizar los efectos causados por un accidente, un usuario o un malware:

- El uso de hardware adecuado frente a accidentes y averías (refrigeración del sistema, conexiones eléctricas adecuadas, etc.)
- La realización de copias de seguridad (backup) de los datos y del sistema operativo en más de un soporte y en distintas ubicaciones físicas.

Contra qué nos debemos proteger

- Contra nosotros mismos, que en numerosas ocasiones borramos archivos sin darnos cuenta, eliminamos programas necesarios para la seguridad o aceptamos correos electronicos perjudiciales para el sistema.
- Contra los accidentes y averias que pueden hacer que se estropee nuestro ordenador y perdamos datos necesarios.
- Contra usuarios intrusos que, bien desde el mismo ordenador, bien desde otro equipo de la red, puedan acceder a datos de nuestro equipo.
- Contra sofware malicioso o malware, es decir, programas que aprovechan un acceso a nuestro ordenador para instalarse y obtener informacion, dañar el sistema o incluso llegar a inutilizarlo por completo

Amenazas

Nuestro ordenador Expuesto a una serie de pequeños programas o software malicioso que puede introducirse en el sistema por medio de los correos electrónicos la navegación por páginas web falsas Etc Podemos encontrar muchos tipos

Tipos de amenazas más comunes

- Virus
- Gusanos
- Troyanos
- Espía
- Dialers
- SPAM
- Pharming
- Phishing

Amenazas: Virus

Programa Se instala en el ordenador Sin el conocimiento del usuario Finalidad Propagarse a otros equipos. Puede provocar desde pequeñas bromas hasta la destrucción total de discos duros.

Amenazas: Gusano informático

Tipo de virus Finalidad Multiplicarse e infectar una red de ordenadores. Consecuencias No suelen implicar la destrucción de archivos pero sí ralentizan el funcionamiento.

Amenazas: Troyano

Pequeña aplicación Escondida en otros programas Finalidad Disponer de una puesta de entrada a nuestro ordenador para que otro usuario o aplicación Recopile información de nuestro ordenador Tome el control absoluto

Amenazas: Espía (spyware)

Programa Se instala en el ordenador sin conocimiento del usuario Finalidad Recopilar información sobre el usuario para enviarla a servidores de Internet gestionados por compañías de publicidad.

Amenazas: Dialers

Amenazas: Spam

Envío de correo electrónico publicitario De forma masiva A cualquier dirección de correo electrónico existente. Finalidad vender sus productos

Amenazas: Pharming

Suplantación de páginas web por parte de un servidor instalado en el equipo sin que el usuario lo sepa. Finalidad Obtener datos bancarios Cometer delitos económicos

Amenazas: Phishing

Obtener información confidencial de los usuarios de banca electrónica mediante el envío de correos electrónicos.

Ingeniería social

Personas revelan información confidencial Delincuente utiliza información para Estafar, realizar compras, etc. Uno de los métodos más efectivos

Estrategias de ingenieria social

Telefonear a los centros de datos fingiendo ser cliente Avisos de falsas compras online Crear sitios web sobre concursos o cuestionarios falsos Buscar en papeleras y alrededores del puesto de trabajo Hacerse pasar por empleado de una empresa

Herramientas

Introducción

- Ya hemos visto en clase que
- Hay amenazas para nuestro ordenador (personas,accidentes,averías,etc) Existen programas,correos o webs que suponen una amenaza (virus, troyanos, phishing...)
- Hoy veremos que herramientas podemos utilizar para detectar o evitar estas amenazas

Tipos de herramientas que veremos:

- Antivirus
- Antiespía
- Firewall

Antivirus

Son programas diseñados para detectar, bloquear y/o eliminar el software dañino. Tienen 2 mecanismos básicos de detección de amenazas: Comparación Buscando entre los programas el patrón de código que coincida con los almacenados en una biblioteca de patrones de virus conocidos. Detección de programas basados en su comportamiento Conoce una serie de comportamientos sospechosos Estudia a los programas que, por su código, estén preparados para llevarlos a cabo.

¿Es importante tener instalado un antivirus?

Es importantísimo! Son algo parecido a nuestros guardaespaldas Se mantienen siempre alerta de posibles programas dañinos que puedan colarse en tu ordenador y hacer uso de los datos y archivos que tienes guardados. Es básico tener instalado un antivirus. ¿Es suficiente tenerlo instalado? ¡No! Se ha de actualizar cada cierto tiempo Cada día aparecen nuevos virus Para poder las últimas “vacunas”

Antispyware (antiespías)

Programas Se encargan de que en tu ordenador no haya programas que roben tus datos. Hoy en día Antivirus tratan de ampliar su protección hacia cualquier tipo de malware Suelen incluir esta función, En ocasioines Es necesario utilizar programas especiales específicos para detectar el spyware complementan la actividad del antivirus. Reflexión antivirus y antispyware De todos modos, ¿cual es la mejor manera de protegerse de estos programas malignos? Ser consciente de su existencia Hacer un uso de la red y del software que minimice el riesgo de que puedan entrar en el sistema. La prudencia es la principal herramienta Extremar la cautela a la hora de enfrentarse a un programa desconocido. No todos los programas que se reciben por correo o se descargan gratuitos de la red están limpios de amenazas. Es importante comprobar y pensar antes de ejecutar.

Software antispam

El spam o correo basura es correo electrónico que se envía masiva e indiscriminadamente por empresas de publicidad. El software antispam son programas basados en filtros capaces de detectar el correo basura, tanto desde el punto cliente(nuestro ordenador) como desde el punto servidor(nuestro proveedor de correo).

Estos filtros analizan los correos electronicos antes de ser descargados por el cliente.La forma de detección esta basada en lsitas o bases de datos de correos spam , en el analisis de la existencia del remitente, etc.

Actualmente la mayoria de los antivirus tienen integrado un filtro antispam.

Firewall (cortafuegos)

Programa encargado de controlar y filtrar las conexiones a red de una máquina Es un mecanismo básico de prevención contra amenazas de intrusión externa. Supone barrera de protección entre un equipo o red privada y el mundo exterior. Controla el acceso de entrada y salida al exterior Filtra las comunicaciones Registra los eventos Genera alarmas.

Funcionamiento

Como un portero Nadie pasará sin que él les dé permiso para hacerlo. Te avisa de posibles programas que quieren hacer algo malo en tu ordenador te hacen invisible ante los posibles ladrones en busca de víctimas. En la web Descargas gratuitas de cortafuegos Es recomendable hacerse con uno Ejercicios privacidad web Abre Internet Explorer, e investiga cómo se eliminan el Historial, las Cookies y los Archivos Temporales. Escribe la secuencia de pasos a seguir para conseguirlo. Realiza las mismas operaciones del ejercicio anterior con Mozilla Firefox. Escribe, de nuevo, la secuencia de pasos a seguir. Ejercicios antivirus Busca en Internet 5 software antivirus y haz una tabla con: El precio que tendría que pagar un usuario particular La página web donde lo podemos encontrar Sus características principales Encuentra 3 antivirus gratuitos en la red. ¿Incluyen Antispyware o Firewall entre sus funcionalidades? Una vez comprado un antivirus, ¿se puede seguir utilizando durante tiempo ilimitado? ¿Por qué? Ejercicios antispyware Busca en la Wikipedia información sobre el programa Spybot-Search & Destroy y contesta las siguientes preguntas: ¿Para qué sirve? ¿Quién lo creó? ¿Cuánto cuesta? Si en una página web encuentras disponible un Antispyware gratuito que dice detectar amenazas graves presentes en tu PC ¿Crees que sería conveniente descargarlo e instalarlo? Justifica tu respuesta.

Ejercicios firewalls

Cuando nos referimos a firewalls también les llamamos “cortafuegos”. ¿Qué es en la naturaleza un cortafuegos?¿Cuál crees que es la relación? Puedes buscar para ello en google. Di si la siguiente frase es Verdadera o Falsa, y justifica tu respuesta: “Internet es la principal fuente de amenazas para la seguridad de un ordenador y, sin embargo disponer de conexión a Internet puede llegar a ser la mejor manera para protegernos”. Investiga cómo se configura el Firewall que viene incluido en el Sistema Operativo Windows. Explica para qué crees que sirven las Excepciones del Firewall

Ejercicios de ampliación 1

Investiga en Internet qué caracteriza el comportamiento de los siguientes tipos de malware Adware: Bloqueador: Bulo (Hoax): Capturador de pulsaciones (Keylogger): Espía (Spyware): Ladrón de contraseñas (PWStealer): Puerta trasera (Backdoor): Rootkit: Secuestrador del navegador (browser hijacker) Ejercicios de ampliación 2 Investiga en Internet el caso de la mayor red zombi desmantelada. ¿Cómo funcionaba dicha red zombi? ¿Con qué finalidad la empleaban? ¿Cómo fue descubierta por las Fuerzas de Seguridad del Estado?