La seguridad TIC en la infancia

PID_00245594

Erik de Luis Gargallo

Material docente de la UOC

Universitat Oberta de Catalunya

Erik de Luis Gargallo

Profesor colaborador del máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones de la Universitat Oberta de Catalunya.

Primera edición: febrero 2017

Av. Tibidabo, 39-43, 08035 Barcelona
Diseño: Manel Andreu
Realización editorial: Oberta UOC Publishing, S. L.

Introducción

Este material pretende ofrecer a sus lectores una introducción general a los riesgos que, hoy en día, presentan para la infancia las tecnologías de la información y las comunicaciones.

Los materiales que ponemos a vuestra disposición se encuentran divididos en tres módulos.

El módulo «Introducción a los fundamentos de la seguridad informática» consiste en una breve introducción al concepto de seguridad informática, observado desde dos puntos de vista: el lógico (o protección del software de un sistema) y el físico (o protección física de los recursos de un sistema).

La reducción o la eliminación de los riesgos asociados a un sistema de información nos lleva a la introducción de los conceptos de confidencialidad, disponibilidad e integridad de los datos, conocidos como la tríada CID. El mantenimiento de estos permite proteger la información contenida en el sistema. Estas tres propiedades serán tratadas en el mismo módulo.

Además, también se explicarán otros conceptos relacionados con la seguridad TIC, como son la autenticidad, la trazabilidad y el no repudio.

El módulo «Software malicioso», como indica el propio título, tiene como objetivo realizar una aproximación a los principales tipos de *malware* existentes.

También se lleva a cabo una clasificación de los principales ataques en el ámbito TIC que se presentan en la actualidad, sobre todo a raíz del considerable uso que se hace de Internet. Se tratarán los ataques de *spoofing* (en sus distintas modalidades), *sniffing*, *phishing*, inyección SQL, *cross-Site scripting*, DoS y DDoS.

Los dos módulos anteriores suponen una introducción básica y esencial para una correcta comprensión del módulo titulado «La seguridad TIC en la infancia. Actuar en el ámbito educativo». En este módulo, considerado el eje del material, se recogen los distintos riesgos que los menores de edad y adolescentes deben tener presentes en su interacción en el espacio digital. En dicho módulo se facilitarán a formadores y educadores las herramientas para afrontar dichos riesgos. Se emplazará a poner un especial énfasis en la educación a través de una cultura de la seguridad eficaz, más allá de recomendaciones de seguridad que combinen el software y el hardware.

Finalmente, y a modo de conclusión, se proporcionarán técnicas y recomendaciones de seguridad orientadas a salvaguardar el funcionamiento normal de nuestros dispositivos, protegiendo nuestros datos sensibles y nuestra privacidad. Se habrá de comprender, por otro lado, el gran desafío que supone mantener el equilibrio entre la sociabilidad y la usabilidad, con la seguridad y la privacidad.

Objetivos

Los objetivos que el alumno ha de alcanzar una vez estudiados los materiales didácticos de esta asignatura son los siguientes:

1. Identificar los objetivos generales de la seguridad informática: la confidencialidad, la integridad y la disponibilidad.

2. Entender los conceptos de seguridad física y seguridad lógica, sus diferencias y las distintas medidas que se pueden aplicar en cada caso.

3. Conocer el distinto software malicioso existente en la actualidad.

4. Identificar los principales tipos de ataques presentes en Internet.

5. Mostrar el estado actual de la relación entre los menores de edad y las tecnologías de la información.

6. Identificar los riesgos más comunes a los que menores y adolescentes deben hacer frente en la actualidad en su relación con las nuevas tecnologías, así como su vinculación con el ámbito educativo.

7. Presentar las recomendaciones de seguridad básicas, tanto para menores como para adultos, en su interacción con el mundo virtual.

Contenidos

Glosario

ActiveX, controles son pequeños programas que se incluyen dentro de las páginas web para dotarlas de mayores funcionalidades, como animaciones o vídeo. Pueden ser objetivo de *malware*.

Actualización del antivirus acción que consiste en la incorporación de la última versión del archivo de identificadores de virus al antivirus, de tal manera que se incluyan todas las características que identifican cada uno de los *malware*, haciendo posible detectarlos y actuar en consecuencia.

Administrador persona o programa encargado de gestionar, realizar el control, conceder permisos, etc., de todo un sistema informático o red de ordenadores.

Adware son programas que muestran publicidad utilizando cualquier tipo de medio, como, por ejemplo, las ventanas emergentes o los *banners*. El usuario puede ser consciente de su instalación y sus funciones, aunque en ocasiones puede que no sea así.

Alias segundo nombre o nombre de pila por el que un determinado *malware* es reconocido. Este alias hace referencia a cierta característica principal del *malware*.

Análisis heurístico técnica utilizada para detectar un nuevo *malware* que en ese momento es desconocido. Una vez que no se ha localizado un malware en el fichero de firmas, mediante esta técnica se ejecuta un análisis de comportamiento en busca de acciones que suele llevar a cabo el *malware*.

Antidebugger conjunto de técnicas que el *malware* emplea para evitar ser descubierto.

***Antimalware*/antivirus** programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador en busca de *malware*.

Archivo de identificadores de *malware* fichero que permite a los antivirus/*antimalware* detectar el *malware*. También es conocido con el nombre de fichero de firmas.

Ataque persistente dirigido o APT ataques silenciosos e imperceptibles cuyo objetivo es una persona o empresa. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de ordenadores. Su peligro consiste en que son ataques personalizados y diseñados especialmente para engañar a las potenciales víctimas.

Backdoor *malware* que se introduce en el ordenador y que establece una puerta trasera a través de la cual es posible controlar el sistema infectado sin el consentimiento por parte del usuario.

Banner anuncio mostrado en una página web que, al ser pulsado, lleva al sitio del anunciante.

Base de datos conjunto de ficheros que contienen datos. También se denomina así al programa o conjunto de programas que gestionan la estructura y la forma con la que dichos datos se almacenan.

Bomba lógica programa en principio inofensivo que puede actuar provocando acciones dañinas.

Bot contracción de la palabra «robot»; es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario.

Botnet red o grupo de ordenadores zombis controlados por el propietario de los *bots*. El propietario de las redes de *bots* da instrucciones a los zombis, como, por ejemplo, la descarga de una nueva amenaza o lanzar ataques de denegación de servicio, entre otros.

Bug término que indica un fallo o error en un programa informático.

Cifrado proceso mediante el cual se codifican la información o los datos de tal manera que resultan inteligibles para un tercero no autorizado. Como técnica, puede ser utilizada por algunos *malware* que se codifican a sí mismos para tratar de evitar que los *antimalware* los detecten.

Cliente sistema informático que solicita servicios y recursos de otro sistema denominado «servidor».

Condición de activación (*trigger*) condiciones bajo las cuales un *malware* se activa y empieza a realizar sus acciones en el ordenador infectado.

Constructor de *malware* programa malicioso que permite crear nuevo *malware* sin necesidad de tener conocimientos de programación, mediante una interfaz a través de la cual se eligen las características del *malware* deseado.

Contraseña cadena de caracteres con la que se restringe o se permite el acceso a un determinado lugar, dispositivo o fichero.

Control remoto acceso al ordenador de un usuario desde otro ordenador que se encuentra en otro lugar.

Cookie fichero de texto que registra la visita de un usuario a una página web y guarda cierta información al respecto.

Cracker persona que rompe o quebranta la seguridad de un sistema informático.

Denegación de servicios distribuida o DDOS ataque de denegación de servicios (DoS) llevado a cabo al mismo tiempo desde varios ordenadores, contra un mismo punto.

Debugger herramienta informática con la que se puede leer el código fuente de los programas.

Sistema de Nombres de Dominio o DNS sistema que facilita la comunicación entre ordenadores conectados a Internet, asignando nombres a las direcciones IP de cada uno de ellos. Los servidores DNS son aquellos ordenadores en los que se relacionan, administran y gestionan todos esos nombres de dominio, y los unen con sus correspondientes direcciones IP.

Denegación de servicios o DoS ataque cuyo objetivo consiste en la inutilización de ciertos servicios de un sistema informático.

Exploit programa que aprovecha una vulnerabilidad existente en un determinado protocolo de comunicaciones, sistema operativo o herramienta informática para conseguir el control remoto de la máquina vulnerada, acceso a sus archivos, etc.

Cortafuegos (*firewall*) protección física o lógica que permite controlar las comunicaciones entre distintas redes, permitiendo a un sistema salvaguardar su información al acceder a estas.

Freeware software gratuito y legalmente distribuido.

Gusano (*worm*) *malware* con la capacidad de realizar copias de sí mismo o de partes de él.

Hacker persona que accede a un ordenador de forma no autorizada. También suele incluir aquellos individuos que detectan y depuran errores en sistemas informáticos.

Hardware término que hace referencia a los elementos físicos de un sistema informático, como la pantalla o los discos duros.

Hijacker programa que cambia la configuración del navegador para hacer que las páginas vistas apunten a otros sitios distintos del indicado por el usuario.

Hoax mensajes de correo electrónico con contenido falso o engañoso, y normalmente distribuido en cadena.

Host término que se refiere a un ordenador que actúa como fuente de información.

***HyperText Transfer Protocol* o HTTP** sistema de comunicación que permite la visualización de páginas web desde un navegador.

***Internet Protocol* o IP** dirección que identifica exclusivamente a cada uno de los ordenadores conectados a Internet.

Java lenguaje de programación que permite generar programas independientemente de la plataforma donde se ejecuten.

JavaScript lenguaje de programación que aporta características dinámicas a las páginas web escritas en lenguaje HTML.

Keylogger programa que recoge y guarda una lista de todas los teclas pulsadas por un usuario, como contraseñas, mensajes de correo, etc.

Malware programa susceptible de causar perjuicios a los usuarios de sistemas informáticos. Proviene de la combinación de las palabras *MALicious* y *softWARE* en inglés.

Nombre común nombre por el que se conoce vulgarmente a un *malware*.

Nombre técnico nombre real de un *malware*, utilizado, además, para indicar su tipo o clase.

Ocultamiento u ocultación (*stealth*) técnica utilizada por algunos *malware* para intentar pasar desapercibidos ante los ojos del usuario afectado y de algunos *antimalware*.

***Peer to peer* o P2P** programas o conexiones utilizadas para el intercambio de ficheros. Algunos ejemplos de estos programas son Emule o Bittorrent.

Parche de seguridad conjunto de ficheros adicionales al software original de un programa informático que sirven para corregir sus vulnerabilidades.

Payload parte del *malware* que realiza la acción maliciosa.

Phishing envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de *phishing* es el envío de correos electrónicos que se hacen pasar por una entidad bancaria en línea para conseguir que el usuario introduzca sus contraseñas en una página web falseada.

Plugin programa que añade nuevas funcionalidades a un determinado programa ya existente.

Polimorfismo técnica utilizada por algunos *malware* para cambiar su firma, de tal manera que resulte diferente en cada ocasión.

Programa espía programas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Denominado *spyware*, puede ser instalado en el sistema sin que medie consentimiento expreso del usuario.

Red grupo de ordenadores o dispositivos informáticos conectados entre sí a través de cable, línea telefónica u ondas electromagnéticas, con la finalidad de comunicarse y compartir recursos entre ellos. Internet está considerada la red de redes.

Hiperenlace (*link*) elementos dentro de una página web que permiten el acceso a otra página o área dentro de la misma página, cuando se pincha sobre ellos.

Réplica acción por la cual los virus se propagan haciendo copias de sí mismos con el único objetivo de realizar posteriores infecciones.

Residente *malware* que se coloca en la memoria del ordenador, de forma permanente, controlando las operaciones realizadas en el sistema.

Rootkit programa diseñado para ocultar procesos, archivos o entradas del registro de Windows cuyo objetivo es mantener la presencia activa de otro *malware* en los sistemas previamente comprometidos. Proviene de la combinación de las palabras *root* y *kit* en inglés.

Script término que hace referencia a los ficheros o secciones de código escritos en algún lenguaje de programación como Visual Basic Script o JavaScript.

Servidor sistema informático que presta servicios y recursos a otros ordenadores denominados clientes, los cuales están conectados en red.

Software ficheros, programas, aplicaciones y sistemas operativos que nos permiten trabajar con un sistema informático.

Spam correo electrónico no solicitado enviado de forma masiva.

***Structured Query Language* o SQL** lenguaje de programación estándar, destinado a la gestión, administración y comunicación de bases de datos.

Troyano programa que llega a un ordenador de forma encubierta, aparentando ser inofensivo. Se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario. La historia mitológica del caballo de Troya ha inspirado su nombre.

***Uníform Resource Locator* o URL** dirección a través de la cual se accede a las páginas web en Internet.

Virus *malware* que se introduce en los ordenadores y sistemas informáticos de formas muy diversas; produce efectos molestos, nocivos e incluso destructivos e irreparables.

Vulnerabilidad fallo de seguridad detectado en un programa que un *malware* podría utilizar para propagar e infectar otros sistemas.

Zombi (*zombie*) ordenador controlado mediante la utilización de *bots*.