Concepto de Seguridad Informática

Tema 1

Álvaro Rodríguez - IES Alonso de Madrigal (Ávila)
2º SMR

Seguridad informática

¿Qué pretende la seguridad informática?

Actualmente se considera aceptado que la seguridad de los datos y la información comprende cinco aspectos fundamentales:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- No repudio

Seguridad informática

Confidencialidad (o privacidad)

Obtener confidencialidad es garantizar que la información sea accesible sólo para aquellos usuarios o sistemas autorizados.

Ejemplo: cifrar un archivo con una contraseña que sólo conocen unos pocos usuarios

Disponibilidad (o accesibilidad)

Asegurar la disponibilidad es conseguir que aquellos usuarios o sistemas con privilegios para acceder a la información puedan hacerlo sin problema durante los periodos de tiempo establecidos.

Ejemplo: implantar sistemas de protección eléctrica en un servidor web

Seguridad informática

Integridad (o confiabilidad)

Mantener la integridad es lograr que la información se conserve tal como fue generada. Es decir, que no se haya manipulado, o bien no se haya corrompido.

Ejemplos: generar un código *hash* para un archivo de datos. Implantar un sistema de copias de seguridad periódicas.

Autenticidad

La autenticidad asegura la identidad del equipo o el usuario que ha generado la información. En ocasiones se emplean terceras partes confiables (**TTP**, *Trusted Third Party*) para autentificar.

Ejemplo: firmar digitalmente un fichero.

Seguridad informática

No repudio (o irrenunciabilidad)

Lograr el no repudio es generar un mecanismo que permita que ninguno de los participantes de una comunicación niegue su participación en la misma. Existen dos tipos:

- **no repudio en el origen:** el usuario o sistema que envía un mensaje no puede negar que lo mandó, pues el receptor tiene mecanismos para demostrarlo. **Ejemplo:** un mensaje firmado digitalmente por el emisor.
- **no repudio en el destino:** el usuario o sistema que recibe un mensaje no puede negar que lo recibió, pues el emisor tiene mecanismos para demostrarlo. **Ejemplo:** un acuse de recibo de un correo electrónico.

Para conseguir el no repudio se cuenta en ocasiones con terceras partes confiables (**TTP**, *Trusted Third Party*).

El no repudio en el origen y la autenticidad son objetivos estrechamente relacionados

Seguridad informática

¿Qué importancia tiene la seguridad informática?

La era de la información es el presente y el futuro de nuestra civilización

Fallos de seguridad → Grandes consecuencias

Ejemplos:

"Cambridge Analytica habría utilizado datos tomados sin permiso (de Facebook) a principios de 2014 para construir una aplicación para predecir e influenciar en las elecciones de EEUU. "

El Ransomware mantiene la supremacía como la principal ciberamenaza de malware en la mayoría de los estados miembros de la Unión Europea, según el informe de Europol, *Internet Organised Crime Threat Assessment* (IOCTA) correspondiente a 2018.

Hace un par de meses se anunció una vulnerabilidad en Google+ que expuso los datos personales de hasta 500.000 usuarios entre el año 2015 y marzo de 2018, cuando la compañía la parcheó.
GitHub sufre el mayor ataque DDoS jamás registrado

+++

Seguridad informática

La Seguridad Completa Es imposible

Actividad:

1. Buscar razones que demuestren que la seguridad total en informática es imposible

2. Busca una noticia reciente (último año) de alguna gran empresa atacada. Recoge la siguiente información:
   - Enlace a la noticia
   - Nombre de la empresa/organización que sufrió el ataque
   - En qué consistió el ataque
   - Quién fue el atacante (Si se conoce)
   - ¿Por qué crees que sufrieron el ataque?¿Qué errores cometieron y quién crees que es el responsable?
   - ¿Cómo se podrían haber defendido ante este ataque?

Seguridad informática

Medidas a llevar a cabo

Personalmente: buenas prácticas, conocimientos, sentido común.

En entornos empresariales y en organizaciones: Además, Planes y Auditorias de seguridad.

Auditorias:

- 2 Tipos: Internas o Externas. En función de quién las realiza. Las externas son más caras pero más completas.
- Abarcan todos los aspectos de la seguridad (CIDAN, lógica y física, etc.)
- Generalmente basadas en estándares de seguridad, como los que veremos más adelante en el tema
- En ocasiones se emite un certificado que demuestra cumplir unos criterios de seguridad

Seguridad informática

¿Qué tipos de seguridad HAY?

- En función del recurso a proteger
  - Seguridad Física**:** protege cada dispositivo o el CPD (Centro de Proceso de Datos) en su conjunto
    - Incendios
    - Inundaciones
    - Robos
    - Apagones y sobrecargas eléctricas
    - …
  - Seguridad Lógica: Protege el software. Las aplicaciones y los datos
    - Confidencialidad
    - Integridad
    - Autenticidad
    - Disponibilidad
    - No repudio

Seguridad informática

¿Qué tipos de seguridad HAY?

En función de cuándo se ponen en marcha las medidas

- Seguridad activa: intenta protegernos de los ataques mediante la adopción de medidas de protección en las interacciones del usuario con el sistema
  - Uso de contraseñas
  - Listas de control de Acceso
  - Encriptación
  - Software de seguridad informática
  - Firmas y certificados digitales
  - Sistemas de tolerancia a fallos en transmisión y almacenamiento de datos
  - Cuotas de disco
- Seguridad Pasiva: Son elementos que, por el simple hecho de integrarlos en el sistema, ya nos protegen de amenazas.
  - Sistema RAID: Redundancia de información para mejorar la integridad y disponibilidad de los datos
  - SAI (Sistema de Alimentación Interrumpida)
  - Copias de seguridad

Seguridad informática

ACTIVIDAD:

Para cada uno de los siguientes supuestos, indica:

- el **tipo de seguridad** empleado según cada uno de los dos criterios
- el/los **objeto/s protegido/s**
- el/los **objetivo/s de la seguridad informática** que se están buscando

a) montar un sistema RAID 1 en un servidor de archivos de una oficina
b) instalar un UPS en una máquina clave de un aula de informática
c) un sistema lector de huellas dactilares para encender un ordenador
d) firmar digitalmente una solicitud de beca
e) generar un SHA-1 de un archivo con una maqueta de Acronis
f) instalar Avast en un equipo recién comprado
g) examinar con SpyBot S&D un equipo en el que saltan muchos anuncios cuando navega por internet
h) usar GnuPG para cifrar con RSA un documento que vas a enviar a alguien

Seguridad informática

Tipos de Amenazas

- Físicas
- Personas
- Software

Seguridad informática

Tipos de amenazas: Físicas

La **seguridad física** cubre todo lo referido a los **equipos** informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red

- **Desastres naturales** (incendios, inundaciones, hundimientos, terremotos). Los tenemos en cuenta a la hora de ubicar el emplazamiento del centro de proceso de datos (CPD), donde alojamos los principales servidores de la empresa
- **Robos.** Nuestros equipos, y sobre todo la información que contienen, resultan valiosos para otros individuos u organizaciones. Debemos proteger el acceso a la sala del CPD mediante múltiples medidas de seguridad: vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc.
- **Fallos de suministro.** Los ordenadores utilizan corriente eléctrica para funcionar y necesitan redes externas para comunicar con otras empresas y con los clientes. Se deben buscar alterantivas ante fallos en los servicios:
  - Segundas conexiones a la red
  - Sistemas SAI (Sistemas de Alimentación Ininterrumpida), contra fallos en la red eléctrica.

Seguridad informática

Tipos de amenazas: PERSONALES

- **Personal de la organización**: a veces amenaza de forma accidental, pero si lo hace de forma intencionada es muy dañino, pues es quien mejor sabe lo que es valioso para la empresa y quien mejor puede conocer la infraestructura y el equipamiento.

- **Ex-empleados**: en numerosas ocasiones aprovechan la falta de mantenimiento de las organizaciones, que no siempre mantienen actualizados los perfiles de acceso a sus sistemas. Un ex-empleado tiene una motivación extra al amenazar un sistema.

- **Hackers**: Los hackers son expertos informáticos en acceder a sistemas protegidos. Los hackers no tienen motivaciones ilícitas ni destructivas, de hecho muchos de ellos son analistas de seguridad. Sin embargo, en su propia labor de análisis y pentesting, aún con fines benévolos, pueden interferir y deteriorar el sistema.

- **Crackers**: son hackers con objetivos perjudiciales o ilícitos. En numerosas ocasiones, contratados para realizar espionaje empresarial.

- **Curiosos**: personas que, en general, realizan ataques pasivos: obtener información sin destruir o modificar la original.

Seguridad informática

Tipos de amenazas: Software

Dos posibilidades:

- Software atacante
- Vulnerabilidades propias del software instalado en el sistema

Seguridad informática

Tipos de amenazas: Software atacante

- Software atacante o Malware:
  - Ransomware
  - Troyano
  - Gusano
  - Spyware
  - MITM
  - Phising
  - SQL injection
  - Rootkits
  - RATS
  - Botnets
  - Ingeniería social
  - Keyloggers.
  - Fuerza bruta.
  - Spoofing.
  - Sniffing.
  - DoS
  - DDoS

Seguridad informática

Tipos de amenazas: Software

- El software está hecho por humanos, luego debemos estar preparados para sufrir los errores introducidos durante su programación. Pueden ser leves (algún mensaje mal traducido), graves (corrupción de datos) y críticos (un agujero de seguridad da acceso libre a datos confidenciales).

- Una **vulnerabilidad** es un defecto de una aplicación que puede ser aprovechado por un atacante. Si lo descubre, el atacante programará un software (llamado **malware**) que utiliza esa vulnerabilidad para tomar el control de la máquina **(exploit)** o realizar cualquier operación no autorizada

Los 5 conceptos de seguridad que debes conocer sí o sí

01 Vulnerabilidad

Agujeros, fallos de programación o implementación que puede ser utilizados para colarse dentro de sistemas o programas.

02 Exploit

Programa o código creado específicamente para aprovecharse de una vulnerabilidad de un sistema o programa.

0-day 03

Vulnerabilidad que no se ha hecho pública y que puede estar utilizándose sin que el usuario sea consciente de ello.

04 Vector de ataque

Los mecanismos utilizados para entrar en los sistemas.

Parche seguridad 05

Desarrollos que corrigen los fallos de seguridad detectados y que impiden que se sigan explotando las vulnerabilidades.

www.osi.es www.incibe.es www.minetur.gob.es

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Seguridad informática

Tipos de amenazas: Software

Tipos de vulnerabilidades:

- **Vulnerabilidades reconocidas** por el suministrador de la aplicación y para las cuales ya tiene un **parche** que las corrige. Si nuestra empresa utiliza esa aplicación, debemos aplicar el parche inmediatamente.

- **Vulnerabilidades reconocidas** por el suministrador, pero todavía **no hay un parche.** En algunos casos sí se proporciona una solución temporal **(workaround),** pero, generalmente, lo mejor es desactivar el servicio hasta haber aplicado el parche.

- **Vulnerabilidades no reconocidas** por el suministrador. Es el peor caso, porque podemos estar expuestos a un ataque durante un tiempo largo sin saberlo. Son los llamados **0-day**

Seguridad informática

ACTIVIDAD

Busca un 0-day que haya salido a la luz en el último mes

- ¿A qué aplicaciones, servicios o dispositivos afecta?
- ¿Con qué código ha sido catalogado? (CVE - ...)
- ¿Ha salido ya un parche para arreglar la vulnerabilidad?
- ¿Has encontrado sitios de internet donde explican cómo explotar esta vulnerabilidad?

Exploit-db.com: página web que recopila muchos exploits y 0-day actualizando día a día

Seguridad informática

Mecanismos de seguridad: Software

Para la confidencialidad:

- programas de cifrado/descifrado
- certificados digitales de clave pública (criptosistemas asimétricos)

Para la integridad:

- herramientas de detección/limpieza de *malware* y virus
- herramientas de cálculo y comprobación de *hash (MD5, SHA-1,etc)*
- programas de *backup* (copias de seguridad)

Para la disponibilidad:

- *software* cortafuegos (*firewall*)
- detección de ataques de denegación de servicio (DDoS)

Para la autenticación:

- *plataformas software para control de acceso*
- *administración de usuarios*
- *certificados digitales (autenticación)*
- *biometría*

Para el no repudio:

- *acuses de recibo*
- *Intermediarios*
- *certificados digitales (firma digital)*

Seguridad informática

Mecanismos de seguridad: Hardware

Para la confidencialidad:

- tarjetas con certificado digital (DNIe u otros organismos)

Para la integridad:

- protectores de corriente (*power surge*)
- dispositivos de copias de seguridad (*backups*)
- analizadores forenses
- detectores de presencia

Para la disponibilidad:

- cortafuegos (*firewall*) *hardware*
- SAIs (suministros de alimentación ininterrumpida)

Para la autenticación:

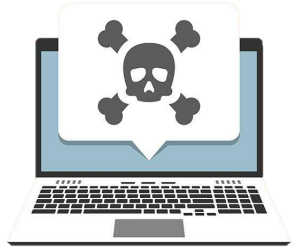
- llaves o tarjetas de control de acceso
- detectores biométricos (huella dactilar, escáner de retina, voz…)

Para el no repudio:

- grabadoras de voz y/o video
- tarjetas con certificado digital (DNIe u otros organismos)

Seguridad informática

Estándares y normativas



- Existen Normativas y Estándares para:
  - Conocer el nivel de seguridad que presentan los sistemas informáticos
  - Definir y diseñar el modelo de seguridad que se desea conseguir
  - Planificar las acciones necesarias para ajustarse a ese modelo.
- Algunos estándares actuales:
  - Estándar Internacional de Buenas Prácticas: ISO/IEC 27002
  - Estándar Internacional con posibilidad de obtención de certificado oficial: ISO/IEC 27001
  - Estándar español de Seguridad Informática: UNE-ISO/IEC 1779

Seguridad informática

¿Qué nos protege de los ataques informáticos?

- La ley: impuesta por los estados
- La buena fe de los que saben: la ética profesional:

"El conocimiento es poder"

"Un gran poder, conlleva una gran responsabilidad"

Debemos utilizar el conocimiento para proteger y no utilizarlo para atacar

Seguridad informática

Legislación relacionada con la seguridad informática

- Como en el mundo real, romper la seguridad informática de una empresa para robar sus datos es un delito perseguido por la ley. También el desarrollo de Internet ha impulsado la aparición de leyes completamente nuevas, como la que regula el comercio electrónico

  - LOPD
  - LSSI-CE
  - LPI

Seguridad informática

Ley Orgánica de Protección de Datos de Carácter Personal

El Real Decreto 1720/2007, de 21 de diciembre, desarrolla la LOPD para ficheros (automatizados y no automatizados). Define tres tipos de medidas en función de la sensibilidad de los datos tratados:

- Nivel básico. Cualquier fichero de datos de carácter personal. Las medidas de seguridad con estos datos son:
  - Identificar y autenticar a los usuarios que pueden trabajar con esos datos.
  - Llevar un registro de incidencias acontecidas en el fichero.
  - Realizar copia de seguridad como mínimo semanalmente.
- Nivel medio. Cuando los datos incluyen información sobre infracciones administrativas o penales, informes financieros y de gestión tributaria y datos sobre la personalidad del sujeto. Las medidas de seguridad incluyen las del nivel básico más:
  - Al menos una vez cada dos años una auditoría externa verificará los procedimientos de seguridad.
  - Debe existir control de acceso físico a los medios de almacenamiento de los datos.
- Nivel alto. Son los datos especialmente protegidos: ideología, vida sexual, origen racial, afiliación sindical o política, historial médico, etc. Las medidas de seguridad amplían las de nivel medio:
  - Cifrado de las comunicaciones.
  - Registro detallado de todas las operaciones sobre el fichero, incluyendo usuario, fecha y hora, tipo de operación y resultado de la autenticación y autorización.

Seguridad informática

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico

Intenta cubrir el hueco legal que había con las empresas que prestan servicios de la sociedad de la información:

- Las obligaciones de los prestadores de servicio, incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones.
- Las comunicaciones comerciales por vía electrónica.
- La información previa y posterior a la celebración de contratos electrónicos.
- Las condiciones relativas a su validez y eficacia.
- El régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

La ley es de obligado cumplimiento para todas las webs que consiguen algún tipo de ingreso, bien directo (pago de cuotas, venta de productos y servicios), bien indirecto (publicidad). La primera obligación que tienen es incluir en su página información de la persona o empresa que está detrás de esa página: nombre o denominación social, dirección postal, datos de inscripción en el registro de la propiedad mercantil, etc.

Seguridad informática

Ley de Propiedad Intelectual

- Establece los derechos de autor en los entornos digitales. Considera la digitalización de un contenido como un acto de reproducción, luego se necesita autorización expresa del titular del contenido.
- Como excepción incluye la copia privada, que es para uso personal del dueño de ese contenido legalmente adquirido. La copia, al igual que el original, no se puede utilizar de manera colectiva ni lucrativa.
- Para compensar a los autores por estas copias no controladas, se establece un canon sobre los distintos dispositivos de almacenamiento. Este canon revierte en las sociedades de autores.

Actividad Final del tema

Consejos de buenas prácticas

Utilizando el contenido visto a lo largo de todo el tema debes preparar la siguiente entrega:

- Un documento de buenas prácticas para usuarios habituales de sistemas informáticos, ya sean ordenadores, teléfonos móviles, tablets... En él debes recoger los aspectos que te parezcan más importantes y se debe presentar de la forma visual, accesible y esquemática posible para que sea útil para los destinatarios.

(Siéntete libre de elegir el formato del documento que prefieras, puede ser: un vídeo, una presentación de diapositivas, un folleto o un cartel a modo de infografía)

Referencias

- Seguridad informática. **José Fabián Roa Buendía**. **McGraw-Hill** España, 2013.
- **Seguridad informática** (Edición 2020) **POSTIGO PALACIOS**, **ANTONIO**. Ediciones Paraninfo, S.A., May 19, 2020