**Seguridad: Tema 1**

1. Visión global de la seguridad informática

La seguridad informática es el conjunto de medidas preventivas y reactivas que protegen los sistemas informáticos y la información que estos contienen

Es imposible garantizar la seguridad de un sistema al 100%

La seguridad se compone de muchos objetivos que se clasifican como principales (CID) o secundarios.

* Confidencialidad: sólo los usuarios autorizados pueden acceder a la información.
* Integridad: garantizar que la información no sufre modificaciones no deseadas.
* Disponibilidad: los usuarios pueden acceder a esta información cuando lo deseen.
* Objetivos secundarios:
  + Autenticidad y control de acceso: comprobar la identidad del usuario que intenta acceder a un recurso y autorizar o denegar el acceso en función de la identidad.
  + Fiabilidad: Basada en la consistencia del sistema con el fin de obtener siempre los mismos resultados de él.
  + No repudio o irrenunciabilidad: garantizar la participación de las partes en una comunicación
    - No repudio en origen: el emisor no puede negar el envío ya que con el mensaje se envía además una prueba que recibe el emisor
    - No repudio en destino: el receptor no puede negar que ha recibido el mensaje ya que cuando este recibe el mensaje se crea una prueba que recibe el emisor
  + Auditabilidad: Registrar el comportamiento del sistema mediante su monitorización.

La estrategia de seguridad se establece mediante políticas y procedimientos que detectan y palian los posibles daños.

La información es el activo primordial que debe protegerse.

En empresas ha de existir un Plan de Seguridad con todos los detalles para proteger el sistema informático.

* 1. **Amenazas, riesgos y ataques**

Amenaza: factor que puede provocar daños a un sistema aprovechando alguna vulnerabilidad

Vulnerabilidad o brecha: grado de exposición del sistema a un ataque.

Contramedida: acción para prevenir una amenaza

Atacante: el autor que realiza la amenaza

Riesgo: Valoración del daño que se puede ocasionar a través de las amenazas teniendo en cuenta las contramedidas que se usan para su defensa.

Tipos de amenazas (dependiendo de la procedencia del agente atacante)

* Amenaza interna: Pertenecen al interior del sistema atacado (empleados) o accidentes.
* Amenaza externa: Proceden del exterior al sistema atacado (robo del servidor o hackeo)

Tipos de amenazas (dependiendo de la via de ataque)

* Amenaza física o ambiental: Aftectan al HW o a las instalaciones (fuego, inundación)
* Amenaza lógica: Afectan al SW mediante la introdución de malware.

**Gestión del riesgo: se puede hacer frente al riesgo de 4 posibilidades:**

* Evitar el riesgo
* Reducir el riesgo
* Retener, asumir o aceptar el riesgo
* Transferir o compartir el riesgo

**Amenazas físicas**

* Personas: la mayoría de ataques provienen de personas que pueden ser malintencionadas o accidentales. Pueden ser atacantes pasivos si sólo fisgonean el sistema, pero no lo alteran o atacantes activos si dañan el sistema o lo modifican a su favor.
  + Personal: cualquier empleado puede resultar una amenaza para el sistema
  + Exempleados: personas que aun no formando parte de la organización la conocen perfectamente
  + Hacker: Persona con altos conocimientos en programación. No tiene por qué ser una persona maliciosa, también puede ayudar a mejorar la seguridad de la empresa
  + Cracker: persona que intenta acceder al sistema con intenciones maliciosas
* Robos, sabotajes, destrucción de sistema
* Cortes, subidas y bajadas bruscas de suministro eléctrico
* Condiciones atmosféricas adversas (humedad alta, temperaturas elevadas)
* Catástrofes naturales o artificiales

**Amenazas lógicas**

* Software incorrecto: Los errores de programación se denominan bugs y existen programas que se aprovechan de estos fallos para atacar el sistema, conocidos como exploits.
* Puertas traseras: los programadores suelen dejar atajos en las aplicaciones que desarrollan las cuales pueden ser aprovechadas
* Bombas lógicas: código de un programa que no se ejecuta hasta que el usuario no las activa. Una vez activas el programa pasa a dañar el sistema
* Virus: código que se inserta en un fichero ejecutable para que cuando el archivo se abra el virus se ejecute.
* Gusanos: programa capaz de ejecutarse y propagarse por sí mismo a través de redes.
* Troyanos: código que se ejecuta a escondidas en un programa sin que el usuario se dé cuenta
* Bacterias: programas que simplemente consumen recursos y se reproducen hasta que el sistema informático queda inutilizado al quedarse sin recursos

**Vulnerabilidades de un sistema (todo componente es vulnerable)**

* Hardware: Por ejemplo desconectar la alimentación de un servidor
* Software: Por ejemplo, un virus puede atacar al sector de arranque en un HDD, SO, etc…
* Datos: estos pueden ser modificados o robados.

Herramientas y procedimientos para controlar y evaluar vulnerabilidades

* Actualizaciones de SO y SW de aplicaciones
* Seguridad en los ficheros y control de acceso de los usuarios a los recursos
* Cuentas de usuario y gestión de contraseñas.
* Registro y auditoría de eventos.
* Configuración de las herramientas de seguridad: antivirus, cortafuegos, copias de seguridad…
* Test de penetración ante ataques internos y externos.
  1. **Planes de seguridad**

La mejor solución contra un ataque es una buena defensa a través de la prevención

Para mantener un sistema seguro hay que seguir las siguientes recomendaciones

* Tener un plan de seguridad que haya sido probado en ocasiones anteriores
* Respetar los códigos éticos a nivel personal y profesional
* Proveer planes de contingencia validados mediante pruebas
* Disponer de un sistema eficaz de evaluación de la seguridad

Toda la información de seguridad y las acciones preventivas y reactivas ante un ataque forman un plan de seguridad (o plan de contingencia). Un plan de respuesta a incidentes tiene 4 fases:

* Acción inmediata para detener o reducir la amenaza
* Investigación del accidente
* Restauración de los recursos dañados.
* Reportar el accidente y los daños a un superior.
  1. **Tecnologías relacionadas con la seguridad en los sistemas**

El administrador cuenta con material variado y en constante evolución para hacer frente a cada vulnerabilidad que pueda surgir. Por ejemplo:

* Cortafuegos
* Administración de las cuentas de los usuarios y los servicios.
* Detección y prevención de intrusos.
* Antivirus y antimalware.
* Infraestructura de clave pública, técnicas de cifrado y firma digital.
* Biometría.
* Redes privadas virtuales.
* Técnicas de seguridad en el comercio electrónico
  1. **Estándares relacionados con la seguridad**

La Legislación provee numerosos estándares con los que trabajar en materia de seguridad informática.

1. Seguridad física y lógica
   1. **Seguridad física y ambiental**

La seguridad física consiste en aplicar contramedidas como barreras físicas o control de acceso físico ante los recursos que se deseen proteger del peligro, ya sea fortuito o no.

El control físico de acceso estudia como el personal puede acceder al sistema. En él se incluye la identificación de los usuarios y también mecanismos automáticos de identificación o registro de los movimientos de estos.

Algunas medidas de seguridad para el control de acceso son:

* Utilizar personal de seguridad y animales
* Detector de metales
* Utilizar sistemas biométricos
* Sistemas de verificación automática de firma
* Sistemas de protección electrónica

La seguridad física mediante el control del ambiente y el control del acceso físico permite disminuir siniestros, generar mayor sensación de seguridad en el trabajo, resolver de manera más clara los incidentes y reducir los riesgos.

* 1. **Seguridad lógica**

La seguridad lógica consiste en aplicar barreras lógicas que protejan el acceso a los datos de personas no autorizadas. Es importante recordar que “todo lo que no está permitido debe estar prohibido”. Es decir, para el administrador el acceso de un usuario tiene que estar expresamente concedido. “Todo lo que no está expresamente concedido está implícitamente denegado”.

Las técnicas de seguridad lógicas buscan los siguientes objetivos:

* Restringir el acceso al Software
* Garantizar a los usuarios el acceso a los recursos que necesita, pero sólo a los que necesita
* Asegurar que se emplean los procedimientos adecuados al tratar la información
* Cuidar la confidencialidad, la integridad y el no repudio en la comunicación de mensaje
* Buscar alternativas para situaciones de fallos en equipos
* Ser capaz de restaurar los sistemas en poco tiempo después de un incidente
* Implementar sistemas de reparto de carga y alta disponibilidad
* Garantizar la continuidad del negocio

El control lógico de acceso se puede aplicar al SO o las aplicaciones.

Es importante que el Plan de Seguridad recoja el procedimiento de como un usuario puede solicitar acceso a un recurso y cómo se concede o deniega dicho acceso.

La NIST (National Institute for Standards and Technology) define los requisitos mínimos de seguridad que necesita cualquier sistema:

* Identificación y Autenticación: Todo usuario debe estar identificado antes de concederle acceso al sistema
* Roles: define las necesidades y obligaciones de los usuarios. En función al rol asignado un usuario podrá disponer de determinados servicios
* Transacciones: Disponer de un procedimiento específico de seguridad para ciertas operaciones delicadas
* Limitaciones a los servicios: procesos que autorizan a los usuarios a disfrutar de los recursos según su rol
* Modalidad de acceso: Define las operaciones permitidas sobre la información (lectura, escritura o ejecución)
* Ubicación y horario: Establece restricciones en función de la ubicación o del horario
* Control de acceso interno: contraseñas, métodos aceptables de cifrado, listas de control de acceso
* Control de acceso externo: Cortafuegos, pasarelas de comunicación, túneles de comunicación
* Administración: Recursos Humanos, organización del personal…
  1. **Niveles de seguridad para sistemas operativos**

Los sistemas siguen el estándar que más le beneficia, pero siguen la referencia del TCSEC. Los fabricantes de estos sistemas evalúan sus productos para establecer el nivel de seguridad según el estándar.

* Nivel D, sin protección
* Nivel C1, protección discrecional: requiere la autenticación de usuario. Permite a un usuario privilegiado controlar el sistema
* Nivel C2, protección de acceso controlado: registra los intentos fallidos de acceso y autorización. Permite varios niveles de autorización (no sólo user y superuser)
* Nivel B1, seguridad etiquetada:
* Nivel B2, seguridad estructurada: capaz de gestionar la herencia de permisos
* Nivel B3, dominios de seguridad: se añade una auditoría exhaustiva de las estructuras de seguridad
* Nivel A1: contiene procesos matemáticos que garantizan la seguridad del sistema.

El estándar europeo está basado en el ITSEC White Book, el cual define 10 funcionalidades (5 equivalentes al TCSEC y 5 orientadas a las aplicaciones)

El estándar de referencia a día de hoy para los fabricantes es el Common Criteria, contiene los siguientes niveles:

* Nivel EAL 1: nivel básico que evalúa la utilización apropiada de las funciones de seguridad, pero no su correcta implementación
* Nivel EAL 2: en este nivel se analiza la funcionalidad del sistema
* Nivel EAL 3: análisis más exhaustivo y a alto nivel de las funciones de seguridad
* Nivel EAL 4: se analiza el sistema a bajo nivel, es decir, la implementación. La mayoría de SO comerciales están a este nivel
  1. **Análisis forense**

El análisis forense establece los procedimientos una vez producido un incidente. Busca información de lo sucedido para poder diseñar una contramedida para que no se vuelva a repetir. También tratar de identificar al agente que realiza el ataque y los daños sufridos. Consta de las siguientes fases.

* Identificación y evaluación del incidente
* Preservación de la incidencia o adquisición de los datos
* Análisis de la evidencia
* Documentación y reporte del incidente