Resumen Tema 1 & 2

Fecha de realización: 9 - 12 - 22

¿Qué proteger?

No nos es posible aplicar todas las medidas de seguridad posibles a todos los equipos de la empresa, deberemos identificar los activos de mayor valor y las medidas a aplicar. El activo más valioso de los equipos es la información.

Equipos:

- No se deben de poder sustraer, ni el equipo ni sus piezas, ni lo que es más importante el disco duro.
- En el caso de los portátiles debemos asegurarnos de que van cifrados al salir de la empresa.
- Hay que destacar que no se deberán introducir equipos no autorizados a la empresa.
- Mediante mantenimiento evitaremos averías.

Aplicaciones:

Los equipos de la empresa solo deben tener las aplicaciones suficientes para llevar a cabo el trabajo asignado. Deberemos evitar instalar software extra porque puede tener vulnerabilidades. Haremos esto mediante maquetación.
El usuario no deberá ser capaz de instalar aplicaciones y/o configurarlas. Deberemos asegurar que el software sea legal.
Es obligatorio instalar un antivirus para curarnos en salud aunque también deberemos de implantar medidas como asignarle pocos privilegios a los usuarios y desactivar el autoarranque de aplicaciones de CD o USB o desactivar estas unidades.

Datos:

Deben de ser protegidos por dos motivos:

- La empresa podría no funcionar con normalidad.
- Pueden llegar a manos de la competencia, pudiendo ser fatal para la empresa.

Los niveles de seguridad deben incluir:

- Que todos los equipos estén protegidos contra software malicioso que pueda robar datos o alterarlos.
- El almacenamiento debe ser redundante.
- Los datos deben estar cifrados para evitar la recuperación de los mismos en manos equivocadas.

Comunicaciones:

Debemos usar conexiones cifradas al conectarnos a otras redes o equipos incluso cuando estemos transfiriendo datos cifrados.

Es recomendable:

- Proteger las conexiones a la red de la empresa ya que debido al teletrabajo las empresas son más vulnerables a ataques.
- También deberemos evitar que cualquier atacante se pueda conectar desde la oficina al conectar el portátil a alguna toma de la pared o a través del wifi de la sala de espera.
- Deberemos evitar el spam y la publicidad.

Objetivos de la seguridad informática

Los principales objetivos de la seguridad informática son:

- Confidencialidad: Es la capacidad de garantizar que la información (ya sea almacenada en el sistema informático o transmitida por red) va estar disponible para las personas autorizadas a acceder a tal información.

  La confidencialidad se intenta garantizar mediante 3 tipos de mecanismos distintos:

  - ➢ Autentificación: Intenta confirmar que una máquina o usuario es quien dice que es.
  - ➢ Autorización: Al ser autenticada, los distintos usuarios tienen distintos privilegios sobre la información (lectura, escritura y modificación).
  - ➢ Cifrado: La información será cifrada para que sea inútil a quien no supere la autentificación.
- Disponibilidad: Se define como la capacidad de garantizar que el sistema y los datos van a estar siempre disponibles para el usuario. Intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido. Para lograrlo se suele sobredimensionar los recursos.
- Integridad: Es la capacidad de garantizar que no se han modificado datos desde su creación sin autorización.
- No repudio: Garantiza la participación de las partes en la comunicación. Intenta lograr que en una comunicación de dos partes intentaremos evitar que cualquiera de ella pueda negar que participara en esa comunicación.

Sabes-tienes-eres

A la hora de autenticarnos podemos clasificar las medidas según 3 criterios:

- Algo que sabes: Deberemos conocer algo que solo nosotros sabríamos. Ejemplo: una contraseña.
- Algo que tienes: Algún objeto que verifique que somos nosotros. Ejemplo: Una tarjeta de radiofrecuencia.
- Algo que eres: Alguna característica física del individuo (biometría). Ejemplo: Huella dactilar.

AAA (Autenticación, Autorización y Accounting)

El accounting se refiere a la información del sistema que está siendo recopilada por el propio sistema. Sirve para establecer limitaciones y penalizaciones. También permiten comprobar la eficacia de las medidas de autentificación y autorización en un análisis forense tras el ataque. Siguiendo el rastro podremos localizar por donde ha entrado el

atacante y resolverlo. Al poder entrar, el hacker puede borrar sus huellas, pero si el registro se hace en otra máquina de manera simultánea ya debe de acceder a ambas máquinas. Generalmente las máquinas de registro suelen tener menos software instalado en ellas por lo que es más dificil acceder a ellas.

E2E (End to end)

Extremo a extremo: Se debe comprobar la seguridad en el origen de los datos, el destino de los datos y el canal de comunicación entre origen y destino.

- En el origen y destino intentaremos que el equipo y las aplicaciones no hayan sido modificados.
- En el canal intentaremos limitar quién accede y sobretodo cifraremos la comunicación porque nuestros datos pasarán por redes externas.

Clasificación de la seguridad:

- Física: Es todo lo referente a los equipos informáticos como los ordenadores, servidores y equipo de red. Las amenazas contra la seguridad física son:
  - Desastres naturales: Deberemos tenerlos en cuenta para ubicar el CPD.
  - Robos: Tendremos que proteger el acceso al CPD con distintas medidas: vigilantes, tarjetas de acceso, identificación...
  - Fallos de suministro: Es recomendable usar baterías o un grupo electrógeno por si falla la corriente o una segunda línea de internet como backup por si hay un corte en la calle.

Amenazas	Mecanismos de defensa
Incendios	• El mobiliario de los centros de cálculo debe ser ignífugo. • Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos. • Deben existir sistemas antiincendios, detectores de humo, rociadores de gas, extintores... para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionado numerosas pérdidas materiales.
Inundaciones	• Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales. • Impermeabilizar las paredes y techos del CPD. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
Robos	• Proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes jurados,...; con todos estas medidas pretendemos evitar la entrada de personal no autorizado.
Señales electromagnéticas	• Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas pues pueden interferir en el correcto funcionamiento de los equipos informáticos y del cableado de red. • En caso de no poder evitar la ubicación en zonas con grandes emisiones de este tipo de señales deberemos proteger el centro frente de dichas emisiones mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
Apagones	• Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida, SAI, que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.
Sobrecargas eléctricas	• Además de proporcionar alimentación, los SAI profesionales incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrica.
Desastres naturales	• Estando en continuo contacto con el Instituto Geográfico Nacional y la Agencia Estatal de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.

- Lógi no de los equipos para garantizar la seguridad del dispositivo.

Amenazas	Mecanismos de defensa
Robos	• Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a la información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafía...).
Pérdida de información	• Realizar copias de seguridad para poder restaurar la información pérdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
Pérdida de integridad en la información	• Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp,... • Mediante la firma digital en el envío de información a través de mensajes enviados por la red.

- **Pasiva:** Son los mecanismos que al sufrir un ataque nos permiten recuperarnos. (Ej: Copias de seguridad)

Técnicas	¿Cómo minimiza?
Conjunto de discos redundantes	Podemos restaurar información que no es válida ni consistente.
SAI	Una vez que la corriente se pierde las baterías del SAI se ponen en funcionamiento proporcionando la corriente necesaria para el correcto funcionamiento.
Realización de copias de seguridad	A partir de las copias realizadas, podemos información en caso de pérdida de datos.

- **Activa:** Son las medidas que adoptamos para proteger los activos de la empresa de ataques. (Ej: antivirus).

Técnicas	¿Qué previene?
Uso de contraseñas	Previene el acceso a recursos por parte de personas no autorizadas.
Listas de control de acceso	Previene el acceso a los ficheros por parte de personal no autorizado.
Encriptación	Evita que personas sin autorización puedan interpretar la información.
Uso de software de seguridad informática	Previene de virus informáticos y de entradas indeseadas al sistema informático.
Firmas y certificados digitales	Permite comprobar la procedencia, autenticidad e integridad de los mensajes.
Sistemas de ficheros con tolerancia a fallos	Previene fallos de integridad en caso de apagones de sincronización o comunicación.
Cuotas de disco	Previene que ciertos usuarios hagan un uso indebido de la capacidad de disco.

Son puertas abiertas para posibles ataques.

Dependiendo de cómo afecten al sistema podemos diferenciarlas en 3 categorías:

- Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las cuales los desarrolladores ya tienen constancia y ya existe un parche para ellas.

- Vulnerabilidades conocidas sobre aplicaciones no instaladas: Son conocidas por los desarrolladores pero ya que no las tenemos instaladas no nos afectan.
- Vulnerabilidades no conocidas (0 days): Aún no han sido detectadas por los desarrolladores, por lo que todos los equipos que tengan descargada esta aplicación son vulnerables.

Clasificación de vulnerabilidades:

Calificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Las definiciones no son 100% adecuadas ya que una vulnerabilidad crítica no tiene por qué ser solamente un gusano.

Tipos de ataque:

El atacante puede elegir alguno de estos tipos de ataque:

- Interrupción: Va a provocar un corte en algún servicio.
- Interceptación: Ha conseguido acceder a nuestras comunicaciones y ha copiado la información.
- Modificación: Ha conseguido acceder pero, en vez de copiar la información la está modificando.
- Fabricación: El atacante se hace pasar por el destino de la transmisión por lo que puede conocer nuestra conversación y hallar información valiosa.

Técnicas de ataque:

A la hora de atacar un activo se puede hacer uso de las siguientes técnicas:

- Ingeniería social: Al poner una contraseña los usuarios pueden recurrir a palabras conocidas como el mes de su cumpleaños, el nombre de su calle, mascota, etc... Si conocemos a esa persona podemos intentar adivinar su contraseña. O podríamos engañar a alguien para que haga algo de lo que podríamos aprovecharnos.
- Phishing: El atacante se pone en contacto con la víctima haciéndose pasar por una empresa con la que tenga relación (bancos, proveedor de internet, etc...) Y en el

contenido del mensaje incita a la víctima a pulsar un enlace para que en una web falsa ingrese las credenciales de la empresa que está suplantando. De esa manera el atacante se hace con las credenciales de la víctima.

- Keyloggers: Un troyano que guarda cada tecla que pulsamos, en busca de usuarios y contraseñas.
- Fuerza bruta: Las contraseñas tienen un número de carácteres los cuales una aplicación puede ir generando todas las combinaciones posibles y probarlas una a una. Se recomienda usar contraseñas largas y no triviales, cambiar la contraseña de vez en cuando y establecer un número de fallos tras el cual se bloqueará el acceso debido a esto.
- Spoofing: El atacante se hace pasar por otra máquina.
- Sniffing: El atacante está en el mismo segmento de red que la víctima y debido a esto tenemos acceso a las conversaciones (por eso es importante que las comunicaciones estén cifradas).
- DOS (Denial Of Service): Consiste en tumbar un servidor saturandolo con muchas peticiones.
- DDOS (Distributed Denial Of Service): Es lo mismo pero con muchas máquinas de alrededor del mundo. Normalmente se debe a que el atacante tiene una botnet con muchos ordenadores secuestrados.

Fases de un ataque:

- Reconocimiento: Obtener información de la víctima mediante distintas herramientas (Ej: OSINT framework).
- Conseguir información del sistema: IP, nombre de host, servicios...
- Obtención de acceso: Búsqueda y explotación de vulnerabilidades.
- Crear una backdoor.
- Borrar las huellas.

Políticas de seguridad:

Son el conjunto de normas y protocolos a seguir donde se definen claramente las medidas a tomar y los mecanismos para controlar su funcionamiento.

LOPD (Ley Orgánica de Protección de Datos):

Hay 3 tipos de medidas para proteger los datos de los usuarios:

- Nivel básico: Cualquier fichero de carácter personal. Las medidas de seguridad con este tipo de datos son:
  - ➢ Identificar y autenticar a los usuarios que puedan trabajar con estos datos.
  - ➢ Llevar un registro de incidencias acontecidas en el fichero.
  - ➢ Realizar copias de seguridad cada semana como mínimo.
- 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:
  - ➢ Cada dos años una auditoría externa verificará los procedimientos de seguridad.
  - ➢ Debe existir un control de acceso físico a los medios de almacenamiento de 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 física y electricidad:

Seguridad de materiales eléctricos	
Recursos frente a fallos en el suministro de energía eléctrica	Solución de seguridad
Grupo electrógeno.	Genera corriente eléctrica independientemente de la corriente eléctrica.
Sistemas de alimentación ininterrumpida (SAI).	Protección frente a variaciones puntuales en el suministro de energía, como picos de intensidad que podrían dañar el sistema y proporciona corriente durante un espacio corto de tiempo a los equipos.
Luces de emergencia.	Iluminan el edificio para poder abandonar el edificio y/o acceder a servidores para apagarlos con normalidad y/o solucionar el problema que causó la avería.

Corriente Monofásica: 1 línea.
Corriente Trifásica: 3 líneas

$$P = V*I$$