MEDIDAS DE PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO

Medidas preventivas contra el malware:

* Suites de seguridad (preventiva y paliativa): es un conjunto de varios programas de seguridad como antivirus, antispyware, antirootkit, antiphishing, antispam, cortafuegos, herramientas de control y protección al navegar como filtros de contenido o control parental, etc. Combaten el malware de dos maneras:
  + Protegiendo el equipo, en tiempo real, contra la instalación de malware, escaneando todos los datos procedentes de la red en busca de malware y bloqueando todo lo que suponga una amenaza.
  + Detectando y eliminando malware que ya ha sido instalado en el equipo escaneando el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en el ordenador.

Las técnicas que utilizan son:

* + Comparación con firmas: se comparan los archivos sospechosos con una base de datos con las firmas de todo el malware conocido hasta la fecha.
  + Métodos heurísticos: también se deduce si el equipo está infectado utilizando técnicas para detectar malware sin tener su firma en la base de datos. Los motores antimalware utilizan:
    - Firmas genéricas: no buscan una coincidencia al 100% pero sí una similitud con una firma, para detectar mutaciones de virus.
    - Desensamblado: se obtiene el código en lenguaje ensamblador del malware y se estudia el código con técnicas conocidas.
    - Desempaquetado: algunos virus han sido empaquetados y comprimidos para evitar que sean detectados. Los antivirus los desempaquetan y analizan.
* Cortafuegos: es un dispositivo software o hardware que forma parte de un equipo o dispositivo de red y está diseñado para proteger dicho sistema bloqueando accesos no autorizados y permitiendo solo los que deban ser permitidos cumpliendo con las directrices definidas en la política de seguridad de la organización.
  + Políticas permisivas: se deniega explícitamente el acceso a la red por parte de algunas aplicaciones, servicios, equipos o redes, permitiéndose el acceso al resto de aplicaciones.
  + Políticas restrictivas: prohíbe el acceso a los recursos del sistema, debiendo autorizarse de forma explícita y caso a caso.

Las reglas son un conjunto de condiciones que deben cumplir los mensajes para que el Firewall permita o rechace su paso. Las reglas suelen tener información como:

* Equipo o red que ha enviado el mensaje
* Dirección IP del equipo o red que recibirá el mensaje
* Protocolo utilizado (TCP, UDP, ICMP)
* Puerto del equipo destinatario o emisor del mensaje
* Acción a realizar sobre el paquete (aceptar, rechazar informando al emisor del motivo por el que se rechazó el mensaje, rechazar sin informar al origen, etc…)

Iptables: es el cortafuegos por defecto de los sistemas Linux y permite filtrar paquetes, realizar tareas de enrutamiento redirigiendo tráfico a equipos concretos, realizar traducción entre dispositivos de red (NAT/PAT) y mantener registros del log.

Medidas paliativas contra el malware:

Constituyen todo el conjunto de acciones que los usuarios realizan para eliminar malware que ha conseguido infectar al equipo.

Las mejores medidas paliativas son las copias de seguridad, el software congelador, los sistemas RAID o las herramientas de recuperación de datos de borrado.

* Copias de seguridad
  + Copias de seguridad del sistema: permiten restaurar un equipo a un estao operacional después de un desastre.
  + Copias de seguridad de datos: permiten restaurar algunos ficheros después de que hayan sido borrados o dañados accidentalmente.
* Software congelador: permite congelar el estado del equipo en el momento determinado, con la configuración y contenidos exactos que el equipo tenía en ese momento determinado. Cada vez que se inicie el equipo el equipo, estará en el mismo estado en el que quedó congelado. Esto proporciona varios beneficios:
  + Se contribuye al anonimato de los usuarios, ya que un usuario malintencionado no puede acceder a información previa a la sesión actual, al borrarse el historial, las cookies y las contraseñas que hayan podido quedar almacenadas por algún descuido.
  + Se protege a los equipos frente a infecciones por software malicioso, ya que durante el proceso de restauración se elimina cualquier malware que haya infectado al equipo.

Centros de protección y respuesta frente a amenazas:

Dos tipos de servicios:

* Preventivos:
  + Avisos de seguridad
  + Búsqueda de vulnerabilidades
  + Auditorías o evaluaciones de seguridad
  + Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras
  + Desarrollo de herramientas de seguridad
  + Propagación de información relacionada con la seguridad
* Reactivos:
  + Gestión de incidentes de seguridad (análisis, respuesta, soporte y coordinación de incidentes de seguridad)
  + Gestión de vulnerabilidades (análisis, respuesta y coordinación de vulnerabilidades detectadas).

Buenas prácticas para protegerse del malware:

* Actualizar el sistema operativo y aplicaciones: actualizar periódicamente el sistema operativo y todas las aplicaciones.
* Protección antimalware: se debe instalar una suite antimalware, así como un cortafuegos y mantenerlos actualizados.
* Cuentas de usuario: usar cuentas de usuario con privilegios limitados para el uso diario del equipo y solo utilizar la cuenta de usuario cuando sea necesario.
* Políticas de seguridad: diseñar políticas que incluyan la definición de contraseñas complejas.
* Datos personales y claves: no facilitar datos personales, ni claves, ni códigos PIN solicitados por correo electrónico u otro medio.
* Precaución al navegar: no navegar por páginas web sospechosas, no confiables o que ofrezcan regalos o promociones dudosas.
* Correo electrónico: se deben observar las recomendaciones expuestas a esta unidad, en el apartado dedicado al correo electrónico.
* Instalación de aplicaciones: se debe tener precaución al instalar o ejecutar programas procedentes de Internet, así como evitar la descarga de software de redes P2P y tener un antivirus.
* Reciclaje constante: los administradores de sistemas deben mantenerse actualizados, suscribiéndose a boletines de seguridad, consultando periódicamente web de información.
* Copias de seguridad: se deben hacer regularmente copias de respaldo a medios extraíbles de los documentos importantes para poderlos recuperar en caso de infección.
* Otras medidas: una realización periódica de auditorías de seguridad y la concienciación de los usuarios en cuestiones de seguridad informática.