T2.2.2 Seguridad del Sistema Operativo

Garantía y Seguridad de la Información.

El problema …

- La arquitectura cliente/servidor es la más extendida en las soluciones IT de todas las compañías.
  - Es imprescindible conocer medidas de **endurecimiento de la seguridad del sistema operativo** para que tanto el cliente como el servidor sean menos susceptibles a ataques contra la seguridad.

La Solución …

- NIST SP 800-123 (2008) recomienda:
  - Planificar
  - Instalar
  - Configurar Actualizar
  - Mantener
    - Tanto el SO como las aplicaciones en uso
  - Todo sistema se organiza en un conjunto de capas:
    - HW / Núcleo SO / Aplicaciones – Utilidades
    - El **endurecimiento de la seguridad debe realizarse en todas esas capas**.
    - Cualquier capa es vulnerable a ataques desde las capas inferiores!!!
  - Buenas prácticas (obligarotias incluso):
    - Australian Signals Directorate, DHS, NSA …
    - Usar sólo aplicaciones aprobadas en la lista blanca
    - Parchear las aplicaciones de terceras partes
    - Parchear vulnerabilidades de los SO y usar las últimas versiones
    - Restringir privilegios administrativos.

Seguridad SO y Aplicaciones: UN PROCESO

- Según señala el NIST 800-123, el proceso de construcción, distribución e instalación de un sistema debe ser un **proceso planificado para minimizar amenazas y mantener la seguridad durante todo el ciclo de vida**.

- EL PROCESO DEBE:
  - Valorar riesgos y Planificar el depliegue del sistema.
  - Asegurar el sistema operativo subyacente y las aplicaciones clave.
  - Asegurar que cualquier contenido crítico esté seguro.
  - Asegurar que se usan los mecanismos de protección de red adecuados.
  - Asegurar que se usan los procesos adecuados para mantener la seguridad.

Planificación de la Seguridad del SO

- Los elementos que deben considerarse son:
  - Propósito del sistema, tipo de información a almacenar, aplicaciones y servicios que proporcionará, requisitos de seguridad.
  - Categorías de los usuarios del sistema, privilegios que tienen y tipo de información que acceden.
  - Cómo se autenticarán los usuarios.
  - Cómo se gestionará el acceso a la información almacenada en el sistema.
  - Qué acceso tiene el sistema a la información almacenada en otros huéspedes (servidores de ficheros o de bases de datos, …) y cómo se gestionará dicho acceso.
  - Quién administrará el sistema y cómo (local, remoto, …) manejará esa administración.
  - Cualquier medida de seguridad que se requiera en el sistema, incluyendo uso de:
    - Cortafuegos
    - Antivirus u otros mecanismos de protección contra malware.
    - Diario de actividades / bitácora (*logging*).

Mejora de la seguridad (Hardening) SO

- NIST SP 800-123:
  - Instalar y parchear
  - Endurecer y configurar el sistema operativo para satisfacer las necesidades de seguridad identificadas:
    - Eliminar servicios, protocolos y aplicaciones innecesarios
    - Configurar usuarios, grupos y permisos
    - Configurar controles de los recursos
  - Instalar y configurar controles de seguridad adicionales
    - Antivirus
    - Cortafuegos de anfitrión
    - Sistemas de detección de intrusos (IDS)
  - Comprobar la seguridad del SO para asegurar que se han tomado las medidas oportunas

Mantenimiento de Seguridad

- NIST SP 800-123:
  - Monitorear y analizar las bitácoras (logs)
  - Realizar copias de seguridad de forma regular
  - Recuperar de acciones que hayan comprometido la seguridad
  - Comprobar periódicamente la seguridad del sistema

Virtualización: Hipervisores

- Virtualización:
  - Tecnología que proporciona una abstracción de los recursos de cómputo usados por el software, que pasa a ejecutarse en un entorno simulado denominado VM (máquina virtual)
- Hipervisor:
  - SW que se sitúa entre el HW y las VMs y actúa como mediador (bróker) de recursos y servicios.
  - Funciones
    - Gestión de la ejecución de las VM: memoria virtual, scheduling, context switching, isolation, …
    - Emulación de dispositivos y control de acceso
    - Ejecución de operaciones privilegiadas para las VM invitadas
    - Gestión del ciclo de vida de las VM: start, stop, pause, shutdown, …
    - Administración de la plataforma y el software del hypervisor.

Virtualización: Alternativas

- Tipo 1: Nativa
  - El hipervisor ejecuta directamente sobre el hardware, sin mediación de otro sistema operativo anfitrión. VmWare
  - El hipervisor controla directamente los recursos hardware y media y orquesta el uso para las VM
- Tipo II: Albergada o de anfitrión
  - El hipervisor es un proceso más de un Sistema Operativo anfitrión (a diferencia del SO invitado que es el que se ejecuta en la VM).
- Container: Virtualización de contenedores o aplicación
  - Un sw llamado contenedor de virtualización corre sobre el SO anfitrión.
  - Proporciona un entorno de ejecución aislado para las aplicaciones.

Virtualización: Seguridad

- NIST SP 800-125:
  - Planificar adecuadamente la seguridad del sistema virtualizado
  - Asegurar todos los elementos y mantener su seguridad:
    - Hipervisor,
    - SO invitados
    - Infraestructura virtualizada
  - Asegurar que el hipervisor esté debidamente asegurado
    - Seguir recomendaciones de un SO estándar.
  - Restringir y proteger de acceso de administrador a la solución virtualizada.
- NIST SP 800-125B (Virtual Networks for VM prot.)
  - Tráfico de gestión:
    - Administración y configuración de la infraestructura virtual
  - Tráfico de infraestructura:
    - Asociado a tareas de mantenimiento (backup, migraciones, …)
  - Tráfico de aplicación:
    - Entre aplicaciones que corren VMs y redes externas
  - Cortafuegos virtuales (Virtual Firewall)