[FORT] TEMA 8: Arquitectura de seguridad de Windows 11

Existen 3 niveles de seguridad:

- Equipos Cliente
- Equipos cliente de Dominio
- Redes Clasificadas (A nivel de fuerzas de seguridad)

Un equipo Windows no se considera un equipo seguro hasta que se ha pagado e instalado una licencia en el equipo. Si se tiene una licencia de Windows 8 o 10, se puede usar para activar Windows 11. Existen 3 tipos de licencia:

- Home: No permite active directory
- Profesional: Centrada en active directory
- Enterprise: Similar a la profesional.

Windows 11 y requisitos de instalación

Windows 11 exige tener un chip TPM 2.0 para cifrado de claves, ademas de una CPU y RAM mínimos. Estos requisitos pueden ser anulados usando rufus para crear el instalador de Windows 11, si se hace esto, las claves de cifrado no serán almacenadas en el TPM, pero el equipo seguirá siendo funcional.

Capa física

La capa física se podría decir que por un lado equivale a cosas de seguridad que se pueden configurar en la BIOS (Contraseña de la BIOS, de donde se arranca, si las teclas de selección de booteo están habilitadas...) Por otro lado, en una caja física se securiza si alguien abre una caja, estableciendo un sistema de alarma que envíe un mensaje de alerta si se ha abierto un equipo.

Seguridad basada en hardware

- TPM 2.0 (Trusted Platform Module): Chip físico que almacena parte de las claves de cifrado y descifrado del equipo. Normalmente una placa base trae 2 chips TMP para tener uno de backup en caso de que falle uno de ellos.
- Arranque Seguro (SecureBoot): Asegura que solo software firmado y certificado se puede arrancar sobre el hardware.
- Virtualización de seguridad (VBS): Utiliza un entorno se parado para ejecutar ciertos programas, generalmente se usa cuando aparece la UAC. Se usan tecnologías de virtualización de hardware para ejectuar operaciones aisladas, protegioendo la memoria.

Seguridad del Núcleo del sistema

- Protección de Código Basada en virtualización (HVCI): Utiliza virtualización para proteger la memoria del sistema operativo contra a taques. Asegura que el código de SO y drivers no sean modificados por malware
- Protección de memoria

Seguridad en sistemas de archivos

NTFS y FAT no ofrecen opciones de seguridad. En la actualidad Fat32 y ExFat se siguen usando. Hay 2 sistemas que permiten securizar estos sistemas de archivos:

- Bitlocker: Permite cifrar el disco duro por completo
- Portección de archivos con EFS (Sistema de Archivos Cifrado): Se usa cuando se quiere compartir una carpeta a través de la red pero no se quiere que pueda acceder cualquiera a esta. EFS permite cifrar una carpeta de red y sus archivos.

Seguridad de red

- Firewall: Windows 11 trae el firewall activado por defecto. Controla todas las conexiones entrantes, aunque suele permitir todas las entradas salientes.
- Protección de Amenazas de Red

Gestión de Identidad

Normalmente se usan nombre de usuario y contraseña pero al no ser seguros existen estos componentes:

- Windows Hello: Permite acceder a través de un Pin, Reconocimiento facial u otros tipos de acceso biométrico
- Autenticación Multifactor (MFA): Se depende de una tercera herramienta como Microsoft Authenticator, Google Authenticator o un sistema de verificación por SMS.

el primer usuario es el 1001, mientras que el adminsitrador tiene ID 500 y todos los usuarios con ciertos permisos altos tienen ID por debajo de 1000

Actualizaciones y Parcheo de Seguridad

- Actualizaciones automáticas: Todos los segundos martes de cada mes se publican los nuevos parches de seguridad. Tiene integración con drivers de hardware. Permite actualizar aplicaciones de microsoft.
- Windows Update for Business : Permite a las empresas gestionar o controlar el despliegue de actualizaciones.

Protección de la privacidad

- Controles de privacidad mejorados
- Transparencia de avisos de Datos

Defensa contra Malware y amenzas

- Microsoft Defender Antivirus: Antivirus integrado en los sistemas windows desde windows 10
- Control de aplicaciones de windows defender (WDAC): Permite a las organizaciones controlar que aplicaciones pueden ejecutarse en sus dispositivos.