Seguridad de BIOS

Transcribed on August 3, 2025 at 9:36 AM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión, en esta sesión vamos a tratar de la seguridad física, vamos a hablar de la BIOS, diferentes opciones de la BIOS, las características de esta y el sistema de arranque y hablaremos también de la inyección de código y de otras opciones relacionadas con la seguridad que tenemos en Avios.

La BIOS es el software que viene diseñado en la placa base y que sirve para localizar y reconocer todos los dispositivos necesarios para cargar el propio sistema operativo.

Algunas medidas de protección para la BIOS es poner una contraseña a la BIOS para que no pueda ser configurada si el usuario no conoce esa contraseña y deshabilitar las opciones de arranque mediante dispositivos extraíbles como puede ser el CUAD o dispositivos USB.

En este entorno es importante la seguridad física, si alguien tiene acceso al dispositivo podría tratar de modificar las opciones de la BIOS o incluso podría abrir el dispositivo y tratar de resetear la contraseña de la BIOS pues extrayendo la pila, lo que pasa que en los equipos más modernos es un poco más dificultoso porque la contraseña de la BIOS se almacena en una memoria auxiliar.

Otro ataque conocido es utilizar las contraseñas de administrador del fabricante que están publicadas en diferentes sitios de Internet y de esta manera poder utilizar esas contraseñas de fabricante para poder restablecer la BIOS a sus valores de fábrica y poder después manipularla.

Algunas herramientas nos van a permitir administrar las contraseñas de la BIOS desde el propio sistema operativo, una de las más populares es DMEO SPVD, requiere privilegios de ejecución porque necesita instalarse como un servicio, tenéis la URL para descargar la herramienta en la diapositiva y también tenéis ejemplos de la sintaxis para utilizar esta herramienta.

Algunas BIOS más modernas van a permitir además proteger el acceso al disco duro mediante una contraseña.

Este tipo de soluciones no cifra el disco duro, lo que hace es que previene el acceso a sistemas compatibles a nivel del driver.

Hay que tener en cuenta que sistemas que no sean compatibles con esta tecnología no serían capaces de reconocer el disco.

These notes were taken with Minutes AI (https://myminutes.ai)

Otro elemento que nos permite el hardware es proteger la inyección de código, para ello tenemos una tecnología que se llama prevención de ejecución de código que varía en función del fabricante, se llama NX, XN, XC o D, El sistema operativo tiene que ser capaz de reconocer esta tecnología del procesador para ser capaz de utilizar Windows reconoce esta tecnología.

Desde Windows XP ServicePack 2 tenemos la posibilidad de activar DEP, pero hay que tener en cuenta que aunque el sistema operativo tenga activado dev y tengamos esa característica disponible en el hardware del equipo, esa tecnología tiene que salir o tiene que utilizarse también a nivel de programación.

El software debe ser compilado para utilizar la tecnología de prevención de reproducción de datos.

Podemos testear si una aplicación utiliza esta tecnología inspeccionando las cabeceras del archivo PE.

Podemos utilizar PSStudio, PE Tools o Explorer Suite.

El administrador de tareas también nos muestra si un determinado proceso tiene activada la protección de ejecución de datos.

Si nos vamos a la máquina virtual, en la máquina virtual vamos al administrador de tareas y en el administrador de tareas nosotros vamos a ver las diferentes aplicaciones que tenemos ejecutándose en el dispositivo.

Si nos vamos a la parte de detalles, podemos seleccionar aquí cualquier proceso y podemos ver las propiedades relacionadas con ese proceso.

Tenemos aquí las opciones de seguridad, el contexto en el que se están ejecutando ese proceso con los permisos de seguridad, información sobre los detalles de la ISO que ha lanzado ese proceso y las versiones previas en el caso de que las hubiera.

Además, desde el administrador de tareas nosotros también podemos ver la localización de la imagen que lanzó ese proceso, bien la librería o bien el ejecutable que lanzó ese proceso.

Incluso podríamos hacer un volcado de memoria de ese proceso para un posterior análisis.

La información que tenemos en el administrador de tareas por defecto es muy pequeña, es muy poquito.

Sin embargo, si vamos a la parte de seleccionar columnas, aquí vamos a poder habilitar que se nos muestre mucha más información.

These notes were taken with Minutes AI (https://myminutes.ai)

Entre toda la información que nosotros tenemos disponible para poder ver podemos seleccionar la virtualización del control de cuentas de usuario o la propia prevención de ejecución de código.

De esta manera, cuando nosotros habilitamos estas columnas automáticamente vamos a ver si tenemos la prevención de ejecución de código habilitada en un determinado proceso.

Como se puede observar, en la mayor parte de los procesos sí que viene habilitada por defecto, es decir, en función que el sistema operativo se ha ido modernizando, estas características de seguridad se han ido aplicando de una forma mucho más general a todos los elementos que se ejecutan en el sistema operativo.

Otras opciones que son interesantes en la parte de la BIOS es el acceso a sistema mediante un password, configurar el orden de arranque.

Algunos fabricantes tienen medidas adicionales o servicios adicionales para proteger el dispositivo.

Y luego dentro de lo que es la parte de hardware tenemos en los dispositivos actuales un chip criptográfico, un chip TPM que podemos utilizar para poder almacenar secretos o certificados digitales o diferentes elementos que se utilizan en medidas de seguridad en el dispositivo.

Por ejemplo, bitlocker utiliza el chip TPM, chip criptográfico cuando nosotros vamos a cifrar el volumen del sistema.

De esta manera guarda las claves de seguridad asociadas a ese cifrado para poder arrancar el sistema operativo.

Algunas opciones que no son necesarias, como por ejemplo el arranque del dispositivo mediante red, podemos deshabilitarlas para que no se puedan utilizar esas características con un atacante para aprovecharse de encender el dispositivo, por ejemplo a través de la red.

Como conclusión, la configuración de la BIOS y es el primer paso para securizar el sistema operativo, pero va a estar condicionada por el fabricante de hardware y por las características disponibles en cada dispositivo.

Conocer bien estas características del dispositivo y configurarlas correctamente es el primer paso para implementar la seguridad de un dispositivo.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.

These notes were taken with Minutes AI (https://myminutes.ai)