Seguridad y Protección en Sistemas Operativos

Sistemas Operativos 2023-2

Armenta Chora Luis Fabian y Sierra Ruiz Nayeli Selene
Profesor Ing. Gunnar Eyal Wolf Iszaevich

1.- Introducción

Asegurar la confidencialidad, integridad y disponibilidad de los datos y recursos del sistema es fundamental en sistemas operativos, y esto se logra mediante medidas de seguridad y protección. La seguridad se centra en prevenir accesos no autorizados, cambios indeseados y pérdida de información. Mientras tanto, la protección se enfoca en separar y controlar los recursos compartidos para evitar que usuarios o procesos no autorizados interfieran o violen dichos recursos.

Es fundamental considerar que la seguridad y protección en los sistemas operativos no solo recaen en los desarrolladores del sistema operativo, sino también en los usuarios y administradores del sistema. Por lo tanto, es importante aplicar buenas prácticas de seguridad, tales como utilizar contraseñas fuertes, actualizar periódicamente tanto el sistema operativo como el software de seguridad, configurar apropiadamente los permisos de acceso y monitorear continuamente el sistema para detectar y responder a posibles amenazas de seguridad.

2.- Tipos de seguridad en sistemas operativos

Podemos encontrar varios tipos de seguridad para proteger los sistemas operativos y los datos almacenados en ellos, a continuación se describen algunos de los más comunes en sistemas modernos:

2.1 Seguridad de autenticación y autorización

La autenticación consiste en garantizar que el usuario sea quien dice ser, es decir, verificar las credenciales brindadas por el mismo gracias a los factores de autenticación las cuales pueden ser:

- Basada en información conocida. Por ejemplo, un PIN o contraseña.
- Basada en posesiones del usuario. Por ejemplo, un código enviado por mensaje de texto SMS.
- Basada en datos biométricos. Por ejemplo, la huella dactilar del usuario.

La autorización son los recursos del sistema a los que el usuario previamente autenticado podrá tener acceso, es decir, verifica los permisos que corresponden a cada identidad [1].

2.2 Seguridad de control de acceso

El control de acceso establece una política de seguridad que define qué usuarios o procesos tienen permiso para acceder a cada recurso del sistema y qué tipo de acceso se les permite.

Un mecanismo de control de acceso actúa como intermediario entre el usuario o proceso y los recursos del sistema, es decir, para acceder al sistema, el usuario debe autenticarse, lo que normalmente implica determinar si tiene permiso para acceder al sistema en primer lugar. Luego, la función de control de acceso evalúa si el usuario puede acceder al recurso específico que solicita. El administrador de seguridad mantiene una base de datos que indica qué recursos y qué tipo de acceso se permiten para cada usuario. El mecanismo de control de acceso consulta esta base de datos para determinar si se otorga el acceso [3].

En general, la seguridad de control de acceso describe la capacidad de un sistema para poder controlar, quién y quién no tiene acceso y a que recursos se tiene entrada.

2.3 Seguridad de cifrado

Seguridad de cifrado es la protección de información sensible o confidencial mediante la transformación de los mismos por medio de algoritmos matemáticos a un formato de cifrado de difícil comprensión, permitiendo así que solo las personas autorizadas con la clave de cifrado puedan tener acceso de nuevo a la forma legible[4]. Los dos tipos de cifrado pueden ser simétricos o asimétricos:

- Simétricos: Se utiliza la misma clave para cifrar y descifrar los datos
- Asimétricos: Se utilizan dos claves, una pública y una privada, la cual no debe ser revelada.

Como podemos ver, la seguridad de cifrado es una herramienta muy útil y esencial a la hora de proteger la privacidad, integridad y confidencialidad de nuestra información sensible, permitiendo así tener una mayor seguridad contra posibles amenazas cibernéticas.

2.4 Seguridad de redes

La seguridad de red en un sistema operativo trata sobre la protección tanto de la información como de los recursos que circulan a través de una red de computadoras. Es decir, la seguridad de redes implica una defensa contra amenazas externas.

La seguridad de redes consiste en lograr la seguridad de red mediante una combinación de herramientas y técnicas de seguridad:

- Autenticación y autorización (Ya antes mencionada)
- Encriptación
- Firewall
- Políticas de seguridad

Es necesario tener en cuenta que los usuarios de la red sean auténticos y con autorización de estar dentro del sistema.

Hoy en día, la seguridad de redes es un tema que debe ser tomado en cuenta debido al incremento en el desarrollo de la tecnología. Es decir, es necesario tener protección en nuestros sistemas para de esta forma evitar el uso indebido de nuestra información y nuestros recursos digitales, por ello, es de gran ayuda estar al pendiente de actualizaciones, softwares nuevos, amenazas de seguridad de redes, entre otros, para saber de qué manera proteger nuestro sistema operativo.

3.- Técnicas de seguridad y protección en sistemas operativos

Las técnicas de seguridad y protección en sistemas operativos son estrategias y medidas que se implementan para salvaguardar la integridad, confidencialidad y disponibilidad de los datos y recursos de un sistema operativo. Algunas de las técnicas comunes y más utilizadas son:

3.1 Software antivirus

Entendemos por software antivirus como aplicaciones o programas diseñados para proteger un sistema informático contra virus, malware y más amenazas informáticas, basados en la detección de los mismos en fase de pre-ejecución cuando aún no se han ejecutado [7]. De forma general su funcionamiento se basa en varios pasos para detectar y eliminar todo tipo de malware.

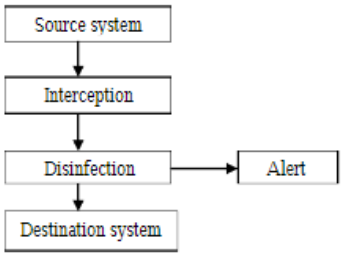

Figura 1. Antivirus

1. Escaneo de archivos y directorios: El antivirus realiza un escaneo en archivos y directorios buscando patrones de virus y malware conocidos para posteriormente compararlos en una base de datos que contiene información de las características de los virus conocidos, si se encuentra una coincidencia se identifica al archivo o programa como malicioso.

2. Análisis heurístico: Algunos antivirus utilizan técnicas heurísticas para detectar malware desconocido o variantes del conocido tales como analizar el comportamiento y características de los archivos en busca de comportamientos sospechosos, como intentos de modificar archivos del sistema, realizar acciones maliciosas o comportarse de forma anormal.[8]

3. Eliminación del malware: Los archivos y programas identificados como maliciosos pueden ser puestos en cuarentena, lo que impide su ejecución o acceso, o ser eliminados del sistema de forma segura, la eliminación de malware permite eliminar los archivos o programas infectados del sistema.

4. Actualización de virus: Es necesario mantenerse actualizados frente a las últimas amenazas conocidas, nuevas definiciones de virus y malware para así poder detectar y eliminar nuevos virus y malware que hayan sido identificados después de la instalación inicial del software.

Es importante tener en cuenta que ningún software antivirus es 100% infalible, es decir, no garantiza una protección absoluta contra todas las amenazas. En conclusión, el uso de software antivirus es importante para proteger nuestros datos ante las amenazas constantes para evitar la pérdida de datos, el robo de información personal y financiera, etc.

Sin embargo, debe ser complementado con prácticas de seguridad sólidas, como contraseñas fuertes, evitar hacer clic en enlaces sospechosos. entre otros.

3.2 Firewalls

Por definición tenemos que el firewall es una herramienta que ayuda a proteger al sistema local y a un red de amenazas de seguridad basadas en la red. En los sistemas operativos, un firewall representa un componente de seguridad el cual examina y filtra el tráfico de red, el cual entra y sale del sistema.

Hoy en día es común y necesario que los sistemas operativos cuenten con un firewall integrado, ya que este representa una técnica para fortalecer la seguridad de nuestro sistema operativo.

Básicamente, un firewall es una forma en la que una computadora especializada está conectada con sistemas que no están dentro de la red, y tiene las medidas de seguridad necesarias para poder proteger la información importante que está dentro de la red. Los firewall alcanzan a estar apoyados en reglas, es decir, se puede establecer reglas para permitir y/o bloquear el tráfico de la red[3].

¿Por qué resulta efectivo un firewall? El firewall resulta ser efectivo debido a que funciona como una barrera de seguridad entre el sistema local y una red externa, mientras permite el acceso a los recursos necesarios. El firewall puede prevenir el spam, y las amenazas de malware, avisando al administrador sobre la actividad no reconocida (sospechosa).

La manera en la que el firewall (cortafuegos) funciona, se basa en detectar en el tráfico de red la amenazas y con la información obtenida, hace una comparación con las reglas para de esta manera poder determinar si la actividad puede ser autorizada o no. Las reglas deben tener palabras clave como “aceptar” y “rechazar” , con esto, la comparación entre el tráfico y las reglas puede ser de una manera más precisa. De igual manera, si se utiliza la palabra clave “descartar” lo que se hace, es bloquear el tráfico sin enviar ningún tipo de respuesta[2].

3.3 Privilegios mínimos

Los privilegios mínimos se implementan mediante la asignación de permisos o derechos de acceso a nivel de usuario o cuenta, esto significa que los usuarios solo tienen acceso a los recursos y acciones necesarios para realizar su trabajo, y no tienen permisos innecesarios que podrían ser utilizados de forma inapropiada, esto siguiendo el principio de privilegio mínimo o de menor privilegio.

El principio de privilegio mínimo nos establece la importancia de restringir privilegios al usuario y solo otorgar aquellos que son necesarios y mínimos para llevar a cabo tareas o funciones específicas. Esto con la intención de reducir la exposición a riesgos y a minimizar la posibilidad de abuso o mal uso de los privilegios, ya que se limita la capacidad de realizar acciones potencialmente dañinas o no autorizadas [9].

Su implementación se puede hacer en diferentes niveles, como el diseño de sistemas, la configuración de permisos de usuarios y la asignación de roles y privilegios. Algunas de las aplicaciones prácticas son:

- Asignación de roles y permisos: Los usuarios y programas deben tener solo los roles y permisos necesarios para llevar a cabo sus funciones específicas, reduciendo el riesgo de que los usuarios realicen acciones no autorizadas o causen daños accidentales o intencionados. Por ejemplo, un usuario que sólo necesita acceder a la información de lectura en una base de datos no debe tener permisos de escritura o eliminación

- Restricción de privilegios de sistema: Los sistemas operativos y aplicaciones deben configurarse con los privilegios más bajos posibles para llevar a cabo sus funciones, limitando la capacidad de los programas maliciosos de comprometer el sistema o acceder a información confidencial. Por ejemplo, un programa que solo necesita leer archivos no debe tener privilegios de administrador.

- Separación de tareas: Los usuarios y procesos deben tener roles claramente definidos y limitados a las tareas específicas que necesitan realizar, reduciendo la posibilidad de errores o acciones malintencionadas al minimizar el alcance de las acciones que un usuario o proceso puede llevar a cabo. Por ejemplo, un usuario que se encarga de la administración de la red no debe tener acceso a la gestión de bases de datos.

- Auditoría y monitoreo: La aplicación también implica llevar a cabo una auditoría y monitoreo adecuado para identificar y detectar posibles violaciones de seguridad. Esto incluye la revisión regular de los roles y permisos de los usuarios, así como el seguimiento de las actividades de los usuarios y procesos para detectar comportamientos sospechosos o no autorizados.

- Defensa en profundidad: También se puede combinar con otras técnicas de seguridad, como la defensa en profundidad, que consiste en la aplicación de múltiples capas de seguridad para proteger un sistema o red. Por ejemplo, además de restringir los privilegios, también se pueden implementar firewalls, antivirus, cifrado de datos (ya mencionados anteriormente) entre otros, como mecanismos de seguridad para proteger aún más el sistema.

Además de reducir el riesgo de ataques y minimizar la exposición a amenazas, los privilegios mínimos también pueden ayudar a mejorar la administración y el mantenimiento del sistema, ya que limitan la cantidad de cambios que los usuarios pueden hacer y facilitan la identificación de problemas y errores.

4.-Conclusión

La seguridad y protección en sistemas operativos son esenciales para garantizar la confianza de los usuarios y la integridad de los sistemas informáticos en general. Es decir, resulta relevante que los usuarios y administradores del sistema apliquen prácticas adecuadas de seguridad, para identificar y responder a posibles amenazas de seguridad.

Esto, debido a que es un asunto en constante progreso que necesita de una atención continua y una actualización frecuente de las prácticas de seguridad para mantener el sistema resguardado de las amenazas de seguridad que evolucionan constantemente.

Fuentes de Consulta

- [1]. Fernández, L. (2020, junio 27). Qué significa autenticación y autorización. RedesZone.https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/
- [2]Ciberseg1922. (2020, 17 septiembre). *Firewall*. Ciberseguridad. https://ciberseguridad.com/servicios/firewall/
- [3].Stallings, W. (2018). Operating systems: internals and design principles (9th ed.). Pearson.
- [4].¿Qué es el cifrado de datos? Definición y explicación. (2022, febrero 11). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/encryption
- [5].Fernández, Y. (2019, 17 octubre). Firewall: qué es un cortafuegos, para qué sirve y cómo funciona. Xataka. https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona
- [6].Security Engineering - A Guide to Building Dependable Distributed Systems. (s. f.). https://www.cl.cam.ac.uk/%7Erja14/book.html

- [7]. Romero Castro, M. I. (2018). *Introducción a la seguridad informática y análisis de vulnerabilidades* (1.a ed.). Area de Innovacion y Desarrollo,S.L. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf
- [8]. Choudhary, S., & Saroha, R. (2013). How Anti-virus Software Works?? (4.a ed., Vol. 3). International Journal of Advanced Research in Computer Science and Software Engineering. https://www.researchgate.net/publication/308800880_How_Anti-virus_Software_Works
- [9]. Principle of Least Privilege (POLP): What, Why & Best Practices. (s. f.). Devolutions. https://webdevolutions.blob.core.windows.net/blog/pdf/principle-of-least-privilege-polp-what-why-best-practices.pdf