Gestión de Seguridad

Juan Pablo Morales, Jhonatan Steven Camacho, Enmanuel Toro Marin

Colegio de Ingeniería de Sistemas, Institución Universitaria Colegios de Colombia

Sistemas Operativos

Uriel Castañeda Sierra

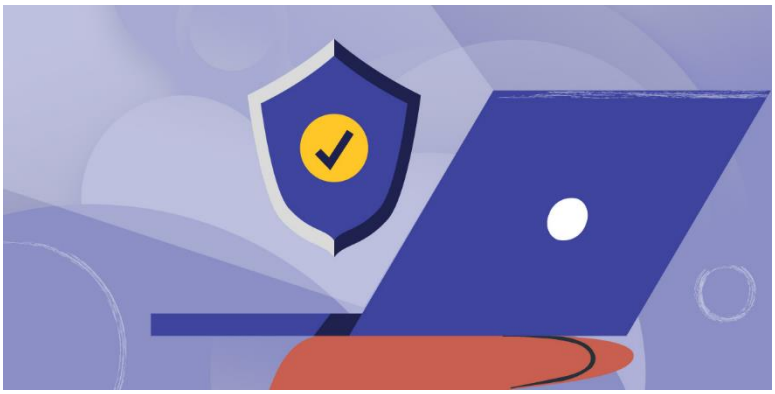
29 de Noviembre de 2023

Índice

Definición

La gestión de seguridad se refiere a las prácticas y medidas implementadas para proteger los sistemas operativos de posibles amenazas y garantizar la integridad, confidencialidad y disponibilidad de los datos y recursos del sistema. Esto implica la implementación de controles de seguridad, como firewalls, antivirus, sistemas de detección de intrusiones, políticas de acceso y autenticación, y la aplicación de parches y actualizaciones de seguridad.

La gestión de seguridad en sistemas operativos es fundamental para proteger los sistemas contra ataques cibernéticos, malware, robo de datos y otras amenazas. También implica la monitorización y el análisis de los registros de seguridad para detectar y responder a posibles incidentes de seguridad.



Estrategias para Control de Seguridad

Estrategias técnicas

Las estrategias técnicas utilizan la tecnología para proteger los sistemas. Algunos ejemplos de estrategias técnicas incluyen:

- Controles de acceso: Los controles de acceso limitan el acceso a los sistemas y recursos a los usuarios autorizados. Algunos ejemplos de controles de acceso incluyen contraseñas, autenticación de dos factores y listas de control de acceso (ACL).
- Cifrado: El cifrado protege la confidencialidad de la información. El cifrado convierte la información en un formato ilegible para los no autorizados.
- Antivirus y antimalware: El antivirus y el antimalware protegen los sistemas de las amenazas de malware. El malware es software malicioso diseñado para dañar los sistemas informáticos.
- Firewalls: Los firewalls protegen los sistemas de las amenazas externas. Los firewalls funcionan como una barrera entre la red interna de una organización y la red externa.

Estrategias administrativas

Las estrategias administrativas se basan en las personas y los procesos para proteger los sistemas. Algunos ejemplos de estrategias administrativas incluyen:

- Educación y capacitación: La educación y capacitación de los empleados sobre la seguridad es esencial para proteger los sistemas. Los empleados deben saber cómo identificar y responder a las amenazas de seguridad.
- Políticas y procedimientos: Las políticas y procedimientos de seguridad establecen las reglas y pautas para proteger los sistemas. Las políticas y procedimientos deben ser claros y concisos y deben aplicarse de forma consistente.

- Supervisión y auditoría: La supervisión y auditoría de los sistemas es importante para detectar cualquier violación de seguridad. La supervisión y auditoría deben realizarse de forma regular y sistemática.

Estrategias físicas

Las estrategias físicas utilizan la seguridad física para proteger los sistemas. Algunos ejemplos de estrategias físicas incluyen:

- Seguridad perimetral: La seguridad perimetral protege los sistemas de las amenazas externas. La seguridad perimetral puede incluir muros, cercas, puertas y cerraduras.
- Control de acceso físico: El control de acceso físico limita el acceso a los sistemas físicos a las personas autorizadas. El control de acceso físico puede incluir sistemas de control de acceso, cámaras de seguridad y guardias de seguridad.
- Almacenamiento seguro: El almacenamiento seguro protege los sistemas y datos sensibles contra el acceso no autorizado. El almacenamiento seguro puede incluir gabinetes de seguridad, cajas de seguridad y bóvedas.

Servicios de Protección y Seguridad

Los servicios de protección y seguridad más comunes en los S. O. incluyen:

- Controles de acceso: Los controles de acceso limitan el acceso a los recursos del sistema operativo a los usuarios autorizados. Algunos ejemplos de controles de acceso incluyen contraseñas, autenticación de dos factores y listas de control de acceso (ACL).
- Cifrado: El cifrado protege la confidencialidad de la información. El cifrado convierte la información en un formato ilegible para los no autorizados.

- Antivirus y antimalware: El antivirus y el antimalware protegen el sistema operativo de las amenazas de malware. El malware es software malicioso diseñado para dañar los sistemas informáticos.
- Firewalls: Los firewalls protegen los sistemas de las amenazas externas. Los firewalls funcionan como una barrera entre la red interna de una organización y la red externa.

Además de estos servicios básicos, los S. O. modernos también pueden incluir funciones de seguridad más avanzadas, como:

- Análisis de comportamiento: El análisis de comportamiento utiliza la inteligencia artificial para detectar actividad maliciosa en el sistema operativo.
- Ingeniería inversa de malware: La ingeniería inversa de malware permite a los investigadores de seguridad comprender cómo funciona el malware y desarrollar defensas contra él.
- Contención de amenazas: La contención de amenazas permite aislar las amenazas del resto del sistema operativo para evitar que se propaguen.

Matriz de Control de Acceso a Recursos

Una matriz de control de acceso a recursos es una herramienta que se utiliza para definir quién tiene acceso a qué recursos y qué acciones pueden realizarse en esos recursos. Se utiliza para ayudar a garantizar que los recursos se utilicen de manera segura y responsable.

Las matrices de control de acceso a recursos se basan en los siguientes elementos:

- Unidades de recursos: Los recursos que se van a proteger. Pueden ser archivos, carpetas, bases de datos, aplicaciones, servidores o cualquier otro recurso al que se acceda de forma electrónica.
- Usuarios o grupos de usuarios: Las personas o grupos de personas que se van a autorizar a acceder a los recursos.
- Operaciones: Las acciones que los usuarios pueden realizar en los recursos. Pueden ser acciones de lectura, escritura, ejecución o modificación.

La matriz de control de acceso a recursos se suele representar como una tabla con tres columnas:

- Unidad de recurso: La primera columna identifica el recurso que se va a proteger.
- Usuario o grupo de usuarios: La segunda columna identifica al usuario o grupo de usuarios que se va a autorizar a acceder al recurso.
- Operaciones: La tercera columna identifica las operaciones que el usuario o grupo de usuarios puede realizar en el recurso.

Ejemplo de matriz de control de acceso a recursos:

	GSUITE	SuperAdmin	Groups Admin	Service Admin	Help Desk Admin	Administrator	User Managment	Member /Standard User	SLACK	Admin	Workspace Owner	Primary Owner	Member / Final User	Guest	ASANA	Admin	Billing Owner	Member	Guest	AWS	UserAdmin	Security Admin	Operator User
Alta Gerencia																							
CEO													x					x					
COO													x					x					
CTO						x	x			x								x			x		
CFO													x					x					
CTIO													x					x					
Tecnología																							
Developers													x					x					
Lider Tecnico										x			x					x					
Operaciones TI													x					x					
Responsable de Infraestructura													x					x					

Las matrices de control de acceso a recursos se pueden utilizar para proteger una amplia gama de recursos, incluidos:

- Sistemas operativos: Los sistemas operativos pueden protegerse mediante la restricción del acceso a los archivos de sistema, las carpetas y las aplicaciones.
- Datos: Los datos confidenciales, como los datos financieros o los datos personales, pueden protegerse mediante la restricción del acceso a las bases de datos, los archivos y los sistemas de almacenamiento.
- Aplicaciones: Las aplicaciones pueden protegerse mediante la restricción del acceso a las funciones y los datos de la aplicación.
- Servidores: Los servidores pueden protegerse mediante la restricción del acceso a los archivos, las carpetas y los servicios del servidor.

Referencias

Fernández, L. (2023, March 16). Control de acceso: qué es y cómo ayuda a proteger nuestros datos. *RedesZone*. https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/

Araujo, A., & Araujo, A. (2023, October 14). Matriz de control de accesos: Qué es y cómo hacerla paso a paso. *Hackmetrix Blog*. https://blog.hackmetrix.com/matriz-de-accesos/