Sistemas Operativos 2

Unidad 5: Seguridad

Conceptos generales

René Ornelis
Primer semestre de 2024

Contenido

Índice de figuras

No table of figures entries found.

Seguridad

1 Protección y seguridad

En esta unidad vamos a estudiar los diferentes aspectos que se deben tomar en cuenta en el diseño y la administración de un sistema operativo, para asegurar que la información siempre esté **íntegra, confidencial y disponible**. En más de una ocasión se nos ha cumplido la ley de fatalidad: en la última hora, antes de entregar el proyecto falla la computadora. Pensemos ¿qué nos duele más: el costo de la computadora o la información que perdimos (y no vamos a poder entregar) o las fotos memorables de las que no tenemos respaldo?

Como vemos, la información se ha convertido en un activo importante para nosotros, que, sin menospreciar el costo de una computadora, la información puede ser irremplazable (como el caso de las fotos) o muy difícil de reproducir.

- **Integridad**: La información debe ser precisa y completa. Esto implica que no se debe modificar sin autorización. Se pueden usar sumas de verificación y hashes para garantizar que los datos no han sido alterados.
- **Confidencialidad**: La información solo debe ser accesible para aquellos que tienen permiso. Esto se puede lograr mediante el uso de cifrado, autenticación y control de acceso.
    - Niveles de confidencialidad
- **Disponibilidad**: La información debe estar disponible para los usuarios autorizados cuando la necesiten. Esto implica proteger los sistemas contra ataques como DDoS y garantizar la redundancia y recuperación ante desastres. La información de una empresa está sujeta a muchas amenazas de software. Los primeros virus y programas malignos fueron producidos por los *script kiddies*: jóvenes entusiastas de la tecnología, que irrumpían en un sistema, sólo para demostrar que podían hacerlo. Actualmente, los autores de programas malignos tienen un objetivo más concreto: información, la cual en la *deep web* pueden vender, y terminan haciendo daño.

Estudiaremos las diferentes amenazas que existen para un sistema y su información y luego los aspectos de diseño y administración que se pueden utilizar para protegernos de los programas malignos.

En cualquier organización, la información es más valiosa que el equipo, aunque, tristemente pocas veces se le da el valor que le corresponde. Lamentablemente los gerentes, y los usuarios en general, muchas veces ven la información o al departamento de tecnología como un gasto o un mal necesario en vez de una inversión, por lo tanto, nos corresponde como profesionales hacer ver el valor de la información, en términos monetarios. Por ejemplo: se puede argumentar que en caso de un ataque perderíamos información y esta información tendría un costo recuperarla, ya sea tiempo fuera de línea por restauración de respaldos o salarios extras porque se tiene que pagar horas extras a operadores para reingresar o recuperar esa información.

También se puede argumentar de si nuestra información confidencial o sensible cae en manos de la competencia, perderemos ventajas lo cual se traducirá en pérdidas financieras; incluso esta información puede usar ser usada como un arma contra nosotros. Esto también se aplica a los individuos.

2 Principio minimalista

La seguridad de un sistema es inversamente proporcional a:

- La cantidad de software instalado
- La cantidad de personas que tienen accesos
- La cantidad de accesos que tengan las personas
- La usabilidad del sistema.

Casos por administrar:

- Gerente “todopoderoso”
- Full Stack Developer

2.1 Gerente “todopoderoso”

Un gerente general que exige tener acceso total a los recursos de TI está centralizando de manera excesiva los privilegios de acceso. Esto significa que una sola persona tiene el control absoluto sobre todos los sistemas, datos y aplicaciones de la empresa. Este modelo de acceso, aunque pueda parecer conveniente a corto plazo, presenta una serie de riesgos significativos para la seguridad informática de la organización.

Riesgos de Seguridad:

1. **Punto único de falla:** Si esta persona sufre algún tipo de compromiso (hackeo, ingeniería social, error humano), toda la infraestructura de TI de la empresa queda expuesta.
2. **Escalada de privilegios:** Un atacante que logra comprometer la cuenta de este usuario podría escalar sus privilegios y obtener acceso a sistemas críticos, lo que facilitaría el robo de datos confidenciales, el sabotaje de sistemas o la toma de control de la infraestructura.
3. **Falta de control:** Sin un sistema de permisos y roles bien definido, es difícil rastrear y auditar las acciones realizadas en los sistemas. Esto dificulta la detección de actividades maliciosas y la investigación de incidentes de seguridad.
4. **Riesgo de abuso de poder:** Un usuario con acceso total podría utilizar sus privilegios para fines personales, como robar datos o realizar cambios no autorizados en los sistemas.
5. **Incumplimiento normativo:** Muchas regulaciones, como el GDPR, exigen un principio de "mínimo privilegio", es decir, que los usuarios solo tengan acceso a los recursos que necesitan para realizar sus tareas. Un acceso total viola este principio.

Centralizar todos los privilegios de acceso en una sola persona representa un riesgo significativo para la seguridad informática de cualquier organización. Es fundamental implementar un modelo de seguridad basado en la minimización de privilegios y en la segmentación de redes para proteger los activos de la empresa.

Lamentablemente, este suele ser el caso para los Gerentes de TI (CIO).

2.2 Full Stack Developer

El caso del Full Stack Developer es similar al del "Gerente Todopoderoso" pero con mayor peligro ya que, al participar en todo el proceso de desarrollo tiene acceso a todos los sistemas y el **conocimiento** para poder hacer daño más preciso y la posibilidad de eliminar todo rastro de sus actividades. Es más, podría fabricar evidencia para inculpar a otros usuarios.

3 Principio del menor privilegio

> *Un usuario debe tener acceso a todo lo que necesita y solamente a lo que necesita para realizar su trabajo.*

4 Áreas de seguridad

Debemos tener en cuenta que la seguridad no es un tema específico de los sistemas operativos ya que los mismos son solo un área en la cual tenemos que buscar la seguridad, como en todos los aspectos de nuestra profesión. Hay varias áreas en las cuales debemos tener la seguridad.

4.1 Área física

La seguridad física consiste en no permitir el acceso al hardware a personal no autorizado. Esta es la primera área en que se debe trabajar implementando estándares de seguridad como:

a) ISO/IEC 27001: Este estándar establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Define un marco para establecer, implementar, mantener y mejorar la seguridad de la información dentro de una organización, incluidos los controles de seguridad física y lógica en un data center.
b) PCI DSS (Payment Card Industry Data Security Standard): Es un conjunto de estándares de seguridad diseñados para garantizar que las empresas que procesan, almacenan o transmiten datos de tarjetas de crédito mantengan un entorno seguro. Incluye medidas para proteger los sistemas de almacenamiento de datos, como el cifrado de datos y la seguridad física del centro de datos.
c) ANSI/TIA-942: Este estándar define los requisitos y las mejores prácticas para el diseño y la operación de un data center, incluida la seguridad física, la infraestructura de red, la energía, el enfriamiento y la gestión de riesgos.
d) Uptime Institute's Tier Standards: Estos estándares definen una clasificación de nivel de disponibilidad para data centers, que van desde Tier I hasta Tier IV, donde Tier IV representa el nivel más alto de disponibilidad. Si bien estos estándares no se centran exclusivamente en la seguridad, la disponibilidad está intrínsecamente ligada a la

seguridad, ya que un data center seguro debe estar diseñado para minimizar el tiempo de inactividad.

e) NIST (National Institute of Standards and Technology): NIST proporciona una serie de documentos, como el NIST Special Publication 800-53, que establece controles y prácticas recomendadas para la seguridad de la información en sistemas de tecnología de la información, incluidos los data centers.
f) SAS 70/SSAE 16/ISAE 3402: Estos estándares se centran en la evaluación de controles de seguridad y procedimientos operativos en un data center. Si bien no son regulaciones de seguridad per se, son importantes para garantizar la transparencia y la confianza entre los proveedores de servicios de data center y sus clientes.
g) HIPAA (Health Insurance Portability and Accountability Act): Para los data centers que almacenan o procesan datos de salud, como registros médicos electrónicos, el cumplimiento de HIPAA es crucial. Este estándar establece requisitos para la protección de la información de salud personalmente identificable (PHI), incluida la seguridad física y lógica.
h) GDPR (General Data Protection Regulation): Si el data center almacena datos de ciudadanos de la Unión Europea, debe cumplir con los requisitos de GDPR en términos de protección de datos personales, lo que incluye medidas de seguridad adecuadas para proteger esos datos.

4.2 Área de usuario

Consiste en educar a los usuarios para no dar información (aparentemente irrelevante) de los sistemas a terceros. Evitar la *ingeniería social.*

> La ingeniería social es una técnica de manipulación psicológica utilizada por individuos o grupos con el fin de obtener información confidencial, acceso no autorizado a sistemas informáticos o realizar alguna acción específica, todo mediante la manipulación de las personas involucradas. En lugar de explotar vulnerabilidades técnicas en sistemas informáticos, la ingeniería social se centra en explotar las debilidades humanas, como la confianza, la credulidad, el miedo o la ignorancia.

Esta técnica puede manifestarse de diversas formas, como llamadas telefónicas falsas, correos electrónicos de phishing, pretextos, suplantación de identidad, entre otros métodos. Un ejemplo común de ingeniería social es cuando un atacante se hace pasar por un empleado de una empresa para obtener información confidencial de otro empleado, como contraseñas o datos de acceso a sistemas.

La ingeniería social es una de las principales amenazas para la seguridad de la información, ya que puede sortear las defensas técnicas más avanzadas si las personas no están lo suficientemente capacitadas para reconocer y resistir los intentos de manipulación. Por lo tanto, la concienciación y la capacitación en seguridad son aspectos fundamentales para mitigar este tipo de ataques.

La capacitación de los usuarios y las pruebas de penetración en este tema debe ser **constante** y debe reflejarse en políticas y normas escritas.

4.3 Área de red

La seguridad de la red se refiere a tener firewalls bien configurados para permitir sólo los ingresos autorizados y para garantizar la seguridad en una red informática, es fundamental implementar una serie de medidas efectivas importantes como:

1. **Cortafuegos (Firewalls)**: Utiliza cortafuegos para filtrar el tráfico de red y proteger la red interna de accesos no autorizados y sistemas de detección de intrusos.
2. **Cifrado de datos**: Cifrar la información sensible tanto en tránsito (usando protocolos como HTTPS, TLS) como en reposo.
3. **Segmentación de red**: Dividir la red en segmentos para limitar el acceso y contener posibles brechas de seguridad.
4. **Control de acceso**: Definir claramente quién puede acceder a qué recursos y aplica el principio de mínimo privilegio.
5. **Monitorización y registro**: Implementar sistemas de monitoreo y registro de actividad para detectar comportamientos sospechosos a través de watchdogs, y responder rápidamente a incidentes.
6. **Red privada virtual (VPN)**: Utilizar VPNs para proteger la comunicación en redes públicas y asegurar el acceso remoto.

Implementar estas medidas ayudará a fortalecer la seguridad de tu red y proteger la información valiosa de posibles amenazas.

4.4 Área de aplicaciones

Los procesos y programas propios de la organización deben contar con sus propias medidas de seguridad independientemente del contexto en que se ejecuten. Los programadores desempeñan un papel crucial en la seguridad de las aplicaciones. Aquí hay algunas medidas que deben considerar para desarrollar software seguro:

1. **Validación de entrada**: Siempre validar y sanitizar la entrada del usuario para prevenir ataques como inyección SQL, XSS y otros tipos de inyección.
2. **Autenticación y autorización**: Implementar mecanismos robustos de autenticación (como contraseñas seguras y autenticación multifactor) y controles de acceso para garantizar que los usuarios solo puedan acceder a lo que les corresponde. De ser posible, la autenticación y autorización debe ser independiente del sistema operativo.
3. **Cifrado**: Utilizar cifrado para proteger datos sensibles tanto en tránsito (con HTTPS/TLS) como en reposo (datos sensibles en la base de datos). Usar algoritmos de cifrado modernos y seguros.
4. **Manejo de errores**: Evitar mostrar información sensible en mensajes de error. Registrar los errores de manera segura para facilitar la depuración sin comprometer la seguridad.

5. **Principio de menor privilegio**: Asignar a cada componente y usuario el nivel mínimo de acceso necesario para realizar sus tareas.
6. **Seguridad en el ciclo de vida del desarrollo (SDLC)**: Integrar prácticas de seguridad en cada etapa del desarrollo, desde la planificación hasta la implementación y mantenimiento.
7. **Revisión de código**: Realizar revisiones de código regulares y auditorías de seguridad para identificar y corregir vulnerabilidades.
8. **Uso de bibliotecas y frameworks seguros**: Utilizar bibliotecas y frameworks que estén actualizados y que sigan buenas prácticas de seguridad.
9. **Seguridad en las API**: Implementar medidas de seguridad en las interfaces de programación (API), como autenticación, autorización y limitación de tasa.
10. **Pruebas de seguridad**: Realizar pruebas de penetración y análisis de vulnerabilidades para identificar y mitigar posibles riesgos.
11. **Mantenerse actualizado**: Estar informado sobre las últimas amenazas y vulnerabilidades en la seguridad de software y actualiza tus prácticas en consecuencia.
12. **Documentación**: Documentar las decisiones de diseño relacionadas con la seguridad y los mecanismos implementados, lo que facilitará futuras auditorías y mantenimientos.

Siguiendo estas prácticas, los programadores pueden contribuir significativamente a la creación de aplicaciones más seguras y resilientes ante posibles ataques

4.4.1 Caso del *single sign on*

El ***Single Sign-On (SSO)*** es un sistema que permite a los usuarios autenticarse una vez y acceder a múltiples aplicaciones o servicios sin tener que volver a iniciar sesión. A continuación, se describen las ventajas y desventajas de utilizar SSO:

Ventajas

1. **Comodidad para el usuario**: Los usuarios solo necesitan recordar una contraseña, lo que reduce la carga de tener múltiples credenciales y mejora la experiencia general.
2. **Aumento de la prductividad**: Al eliminar la necesidad de iniciar sesión repetidamente en diferentes aplicaciones, los usuarios pueden acceder rápidamente a los recursos que necesitan, mejorando la eficiencia.
3. **Mejor gestión de contraseñas**: Fomenta el uso de contraseñas más seguras, ya que los usuarios pueden centrarse en crear una contraseña fuerte en lugar de múltiples contraseñas débiles.
4. **Centralización de la autenticación**: Permite a los administradores gestionar y controlar el acceso a múltiples aplicaciones desde un único punto, facilitando la administración de usuarios y permisos.
5. **Facilidad de integración**: Muchas soluciones SSO son compatibles con estándares como SAML o OAuth, lo que facilita la integración con aplicaciones existentes y servicios en la nube.
6. **Mejora de la seguridad**: Al reducir el número de contraseñas que los usuarios deben gestionar, se minimizan las posibilidades de que utilicen contraseñas débiles o repetidas.

Desventajas

1. **Punto único de fallo**: Si el sistema SSO falla o es comprometido, el acceso a todas las aplicaciones y servicios conectados puede verse afectado, lo que puede interrumpir la operatividad.
2. **Dependencia de un proveedor**: Si se utiliza un servicio SSO de terceros, la organización depende de la seguridad y disponibilidad de ese proveedor.
3. **Desafíos de implementación**: Integrar SSO con aplicaciones legadas o que no son compatibles puede ser complicado y requerir un esfuerzo significativo.
4. **Gestión de sesiones**: Si un usuario se desconecta de una aplicación, puede que no se desconecte automáticamente de todas las demás, lo que podría presentar riesgos de seguridad.

En general, ante el uso forzado de SSO, lo recomendable es:

- Obligar la reautenticación al ingresar a una aplicación o servicio
- Usar sesiones por aplicación que se cierren después de cierto tiempo de inactividad

4.5 Área del sistema operativo

El sistema operativo se convierte en la última línea de defensa para asegurar la información. Para esto se deben tomar diversas medidas, entre las cuales están:

1. **No utilizar la configuración de fábrica**: En los sistemas de uso general, las instalaciones de fábrica incluyen una gran cantidad de software y configuraciones que nunca se usarán (*bloatware*) y se convierten, además de espacio y memoria desperdiciada, en una vulnerabilidad. Una medida primaria es desactivar y desinstalar servicios y aplicaciones no utilizados:
2. **Mantén el sistema operativo actualizado**: Se debe instalar todas las actualizaciones de seguridad y parches disponibles de manera oportuna.
3. **Activa el cortafuegos**: Configurar y habilitar el cortafuegos integrado para filtrar el tráfico entrante y saliente.
4. **Control de usuarios y privilegios**
    a. **Crea cuentas de usuario limitadas**: Utilizar cuentas de usuario con privilegios mínimos y evitar el uso de cuentas administrativas para actividades cotidianas.
    b. **Implementa el principio de menor privilegio**: Asignar solo los permisos necesarios a cada usuario y aplicación.
5. **Seguridad de contraseñas**
    a. **Políticas de contraseñas robustas**: Establecer requisitos para contraseñas seguras (longitud, complejidad, caducidad).
    b. **Uso de autenticación multifactor (MFA)**: Siempre que sea posible, implementar MFA para añadir una capa adicional de seguridad.
6. **Cifrado de datos**
    a. **Cifra datos sensibles**: Utilizar herramientas de cifrado para proteger datos en reposo y en tránsito, especialmente para información confidencial.
7. **Auditoría y registro**

a. **Habilitar la auditoría y el registro de eventos**: Configurar el sistema para registrar eventos críticos de seguridad y accede regularmente a estos registros para detectar actividades sospechosas.

8. **Protección contra malware:** Instalar y actualizar software antivirus/antimalware:
9. **Respaldo regular de datos:**: Realizar copias de seguridad periódicas de los datos críticos y verifica que se pueden restaurar correctamente.
10. **Desactivación de comparticiones innecesarias:** Desactivar las comparticiones de archivos o recursos que no sean necesarios.

4.5.1 Caso de FreeBSD

- Enfocado en seguridad
- Instalación mínima

5 Amenazas de seguridad

En los primeros días de Internet, los *crackers* hicieron noticia al irrumpir en los sistemas de empresas y organizaciones, y desde entonces se inició el tema de la seguridad de los sistemas de información. Sin embargo, el tema no era tan crucial, ya que la mayoría de los *crackers* tenían como objetivo principal demostrar que podían hacerlo. Ya no es así, hoy las violaciones de seguridad tienen objetivos más específicos: robar información, principalmente de tarjetas de crédito y cuentas bancarias, apoderarse de las computadoras para uso posterior o dañar los sistemas de un competidor.

Estos posibles ataques a la información, nos debe mantener alertas sobre las formas en que debemos protegernos. Por lo tanto, debemos distinguir entre los diferentes tipos de ataques.

5.1 Virus

- Programas
    - Autoreplicables
- Daño de información
    - Diversidad de objetivos

5.2 Ransomware (secuestro de información)

- Programas
- Encriptación de información
- Pago por la llave de desencripción

5.3 Botnet (roBOT NETwork)

Hacer uso del poder de cómputo de nuestro equipo remotamente para fines diversos. El uso común es envío de correo de publicidad no solicitados (spam) y los ataques de denegación de servicio distribuidos (DDOS). Actualmente, con el auge de las criptomonedas, ha surgido una nueva variante: la **criptominería**, que consiste en usar nuestra máquina para hacer minería de criptomonedas, sin nuestro consentimiento y, obviamente, sin participar de las ganancias.

5.4 Phishing

- Sitios en Internet
- Suplantación de entidades
    - Bancos
    - Correo electrónico
    - Sitios de juegos

5.5 Scam (ingeniería social)

- Sitios o mensajes de correo electrónico
- Estafa
    - Transferencias
    - Compras fraudulentas

6 Medidas básicas de seguridad

Por lo cual vamos a repasar algunos temas o acciones básicas que podemos tomar para asegurar nuestras computadoras y sobre todo para educar a nuestros usuarios ya hay cosas tan simples que que en realidad cualquiera lo puede hacer no se necesita un conocimiento técnico avanzado para protegerse verdad son solo cuestión de tomar medidas básicas

- Reconocimiento de sitios
    - Referencia conocida
    - Prestigio
    - Búsqueda de “quién es”
    - https://www.mywot.com/
- Certificados de seguridad
- Verificación de nombre
- Verificación de enlaces

7 Referencias

https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/pruebas-sobre-ciberseguridad