Universidad de Guadalajara

Centro Universitario De Ciencias Exactas E Ingenieritas CUCEI

Ingeniería Informática

Actividad 16 – Seguridad

Juan Antonio Ramírez Aguilar

Código: 212482507

Mtra. Becerra Velázquez Violeta del Rocío

Seminario de Solución de Problemas de Uso, Adaptación, Explotación de Sistemas Operativos

Indicé

I. Introducción

El ámbito de la seguridad informática es amplio y a menudo implica una mezcla de tecnologías y soluciones de seguridad. Trabajan conjuntamente para hacer frente a las vulnerabilidades de los dispositivos digitales, las redes informáticas, los servidores, las bases de datos y las aplicaciones informáticas.

Los ejemplos más citados de seguridad informática incluyen disciplinas de seguridad digital, como seguridad endpoint, seguridad en la nube, seguridad de red y seguridad de aplicaciones. Pero la seguridad de TI también incluye medidas de seguridad física (por ejemplo, cerraduras, tarjetas de identificación, cámaras de vigilancia) necesarias para proteger edificios y dispositivos que albergan datos y activos de TI.

Por qué es importante la seguridad informática

Los ataques cibernéticos y los incidentes de seguridad pueden cobrarse un precio enorme medido en pérdidas de negocio, reputación dañada, multas reglamentarias y, en algunos casos, extorsión y robo de activos.

Por ejemplo, el informe Costo de una filtración de datos 2023 de IBM estudió más de 550 empresas que sufrieron una filtración de datos entre marzo de 2022 y marzo de 2023. El costo promedio de una filtración de datos para esas empresas fue de 4,45 millones de dólares, un 2.3 % más que los hallazgos de un estudio similar realizado un año antes, y un 15.3 % más que en un estudio de 2020. Los factores que contribuyen al costo incluyen todo, desde notificar a clientes, ejecutivos y entes reguladores hasta multas normativas, ingresos perdidos durante el tiempo de inactividad y clientes perdidos permanentemente.

II. Seguridad en Sistemas Operativos

La seguridad del sistema operativo se refiere a la protección de las aplicaciones y los recursos de hardware de un sistema operativo contra diversos ataques maliciosos, como el acceso no autorizado, la manipulación de código y la suplantación de identidad. Implica la implementación de políticas de seguridad, control de acceso, mecanismos de autenticación y el uso de criptografía para garantizar la confidencialidad e integridad de los datos. Las políticas de seguridad obligatorias, controladas por un administrador de políticas de seguridad del sistema, desempeñan un papel crucial para garantizar la seguridad del sistema operativo. Las aplicaciones de confianza con privilegios especiales se limitan al nivel mínimo de privilegios requerido para sus funciones a fin de minimizar los riesgos de seguridad.

Las medidas de seguridad de los sistemas operativos que analizamos en este capítulo son de uso común en empresas de todo el mundo. Los diversos pasos que repasamos al hablar del fortalecimiento de los sistemas operativos suelen ser implementados por cualquier organización competente que esté construyendo servidores para su implementación, especialmente cuando estos servidores estarán conectados a Internet. Esto depende de la organización en cuestión y de su estrategia de seguridad.

El uso de herramientas antimalware, HIDS y firewalls de software también es bastante común en muchas organizaciones de cualquier tamaño. Es común ver herramientas antimalware instaladas en servidores proxy que filtran el tráfico web y de correo electrónico que entra desde Internet. Sin estas herramientas, incluso con una seguridad fronteriza muy sólida mediante firewalls e IDS, si algo logra eludir estas medidas, causará graves problemas en nuestras redes internas.

Las herramientas que analizamos en este capítulo y en el Capítulo 10 son esenciales para la industria de la seguridad. Una gran cantidad y variedad de estas herramientas pueden utilizarse en cualquier entorno para diversos usos, pero dedicar tiempo a aprender algunas de las más comunes, como Nmap y Nessus, será útil para quienes se inician en el sector de la seguridad. Si bien es posible que veamos herramientas comerciales más grandes y costosas en uso en un entorno determinado, a menudo se utilizan junto con las herramientas más tradicionales.

Además de garantizar que el sistema operativo de su sensor esté actualizado, es fundamental que se base en las mejores prácticas de configuración segura incluso antes de instalar el software del sensor. Existen varios enfoques para las mejores prácticas de seguridad del sistema operativo . Si su organización cumple con algún tipo de estándar de cumplimiento formal, como HIPAA, NERC CIP o PCI, es probable que ya empleé algún tipo de estándar de configuración segura del sistema operativo. Las agencias federales y del sector de defensa también están familiarizadas con estos estándares, ya que la seguridad del sistema operativo se garantiza mediante diversos procesos de certificación y acreditación.

III. Seguridad en la Red

La seguridad de red es un campo de la ciberseguridad que se centra en proteger las redes informáticas y los sistemas de comunicación de ciberamenazas y ciberataques internos y externos .

Hoy en día, las redes informáticas forman la columna vertebral de la mayoría de las compañías modernas, desde las herramientas de comunicación y colaboración de los empleados hasta aplicaciones complejas (aplicaciones), operaciones nativas de la nube de negocios y hasta infraestructura global. Las redes modernas y las herramientas y soluciones que las mantienen seguras son críticas para el éxito de algunas de las empresas más grandes y exitosas del mundo.

Según un informe reciente, el mercado global de soluciones de seguridad de red es sustancial y crece a un ritmo saludable. En 2024, valía USD 24 mil millones y se espera que Continuar creciendo a una tasa de crecimiento anual compuesta (CAGR) del 14 % hasta alcanzar USD 73 mil millones en 2032.

¿Qué es una red informática?

Las redes informáticas, o simplemente redes, son sistemas de dispositivos interconectados que se comunican entre sí, comparten datos e intercambian recursos. Los dispositivos conectados a través de una red utilizan varias conexiones, incluidas Ethernet, inalámbricas (wifi) y celulares. Después de establecer una conexión, deben seguir un conjunto de reglas conocidas como protocolos de comunicación que rigen la forma en que intercambian datos. Los dispositivos comunes utilizados en redes informáticas incluyen computadoras de escritorio, dispositivos móviles y enrutadores.

Hoy en día, las redes informáticas sustentan casi todos los aspectos de la vida diaria, desde empoderar a la fuerza laboral móvil hasta apuntalar las redes sociales y potenciar el sistema financiero global. Cuando se infringen, es costoso.

Mejores prácticas de seguridad de red

Segmentación de la red de práctica

La segmentación de red, la práctica de dividir una red en segmentos más pequeños permite a las organizaciones implementar un mayor control sobre los datos y los usuarios de una red. La segmentación de la red reduce el tamaño de la superficie de ataque y la cantidad de formas en que los piratas informáticos pueden obtener acceso no autorizado.

Implemente la autenticación multifactor (MFA)

La autenticación multifactor (MFA) es una forma de verificar la identidad de un usuario a través de al menos dos formas distintas de prueba, como una contraseña y una identificación facial. En seguridad de red, MFA proporciona una capa adicional de protección además de la contraseña del usuario que puede evitar que actores maliciosos obtengan acceso a datos confidenciales.

Use redes privadas virtuales (VPN)

Las redes privadas virtuales (VPN) son servicios que establecen conexiones seguras y encriptadas para intercambiar datos y recursos a través de Internet. La seguridad de la red se basa en las VPN para enmascarar las direcciones, la ubicación de un dispositivo en una red para que la actividad de un usuario sea más difícil de rastrear.

Las VPN han desempeñado un papel crítico en la evolución del trabajo remoto, permitiendo a los usuarios acceder a la información y los recursos de la empresa desde cualquier parte del mundo. Este acceso incluye trabajar a través de redes wifi públicas en lugares como cafeterías u oficinas via satélite.

Cree un marco de confianza cero

La confianza cero, una estrategia de seguridad moderna diseñada para la nube, se centra en proteger las conexiones de usuarios individuales a una red en lugar de otorgar confianza implícitamente a todos los miembros.

Antes de la expansión de la computación en la nube, la seguridad de las redes se centraba en proteger los endpoints, es decir, los dispositivos que se conectaban a las redes e intercambiaban información, pero este enfoque no resultaba tan eficaz en un entorno de nube.

Capacitar y evaluar a los empleados regularmente

Las mejores soluciones y sistemas de seguridad de red solo son eficaces si los equipos encargados de implementarlos reciben capacitación periódica y se someten a pruebas rigurosas.

Las organizaciones deben asegurarse de que los usuarios de una red estén familiarizados con sus políticas de seguridad, también conocidas como protocolos de seguridad. También deben comprender los pasos a seguir cuando sospechan que se está produciendo una filtración de datos.

IV. Seguridad de usuario

La gran parte de acciones y tareas que realizan las empresas genera un gran volumen de información confidencial recogida en forma de distintos documentos: una factura, una orden de compra, una orden de pago, nóminas, etc. Implementar las 9 medidas de seguridad informática es de vital importancia para que nuestra empresa pueda trabajar de forma correcta y para que cumpla con las normativas vigentes sobre protección de datos.

Controles de acceso a los datos más estrictos

¿Cómo proteger la información de una empresa? Una de las principales medidas de seguridad es limitar el acceso a la información. Cuantas menos personas accedan a una información, menor será el riesgo de comprometerla. Por lo tanto, es necesario implantar en nuestra empresa un sistema que impida dar acceso a datos innecesarios, a un usuario, cliente, etc.

Realizar copias de seguridad

Poseer un sistema de copias de seguridad periódico permite que la empresa garantice que puede recuperar los datos ante una incidencia de carácter catastrófico, impidiendo la pérdida de estos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos.

Utilizar contraseñas seguras

El acceso a las distintas plataformas que utiliza la empresa (correo electrónico, servidor de copias de seguridad NAS, etc.) debe realizarse utilizando claves de seguridad (contraseñas) seguras, que impidan que puedan ser fácilmente descubiertas por piratas informáticos. El uso de contraseñas seguras es una de las medidas de seguridad informática más importantes en una empresa.

Proteger el correo electrónico

Hoy en día, la mayoría de las comunicaciones de nuestra empresa la realizamos utilizando el correo electrónico. Por lo tanto, otra medida de seguridad es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.

Contratar un software integral de seguridad

¿Cómo proteger la información en internet? La mejor forma es contratando un paquete de seguridad integral que contenga antivirus, antiespías, antimalware, firewall, etc., y que permita proteger la información ante posibles ataques externos a través de internet.

Utilizar software DLP

Existen programas de prevención de pérdidas de datos (DLP) que pueden ser implementados como medida de seguridad en nuestra empresa para supervisar que ningún usuario esté copiando o compartiendo información o datos que no deberían.

Trabajar en la nube

Trabajar en la nube permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor será responsable de esa seguridad.

Involucrar a toda la empresa en la seguridad

Para que las medidas de seguridad informática de una empresa funcionen, debemos involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes, proveedores, etc. Muchas veces, nuestra empresa tiene implantados los sistemas correctos de seguridad, y la brecha en la misma, se produce al relacionarnos con un tercero que carece de estas medidas de seguridad.

Monitorización continua y respuesta inmediata

Debemos implantar en nuestra empresa un sistema que permita monitorizar la gestión de los datos y detectar aquellos posibles fallos o actuaciones incorrectas. Este sistema de control permitirá actuar rápidamente para solventar cualquier incidencia y minimizar su repercusión.

V. Documental vista: Zero Days

En el documental sigue la historia del Stuxnet, un virus diseñado en 2010. Pro a diferencia de otros virus, este buscaba crear daño real. Los expertos en el documental explican que posiblemente el objetivo del virus era el programa nuclear Irani, en específico un planta de tratamiento nuclear.

Este virus era capaz de ingresar en sistemas aislados y reprogramar desde adentro para generar caos. En el documental, se explica que el virus fue creado entre Estados Unidos e Israel, usando por primera vez software como arma de guerra.

VI. Conclusión

En esta actividad aprendí un poco de seguridad informática. Desde lo sistemas operativos y como herramientas como el firewall lo protegen, a las redes y como los protocolos ayudan a mitigar las infiltraciones de red. Pero lo mas importante creo yo que es la seguridad que el mismo usuario maneja. Esto el lo mas importante, ya que actualmente los hackers suelen apuntar más a los usuarios que tratar de romper los sistemas de seguridad de las plataformas.

Nunca esta de mas un curso de seguridad informática y más en un país donde parece no importarles la seguridad de sus sistemas, incluso lo hemos visto en el gobierno mismo.

VII. Referencias

- Flinders, M., & Smalley, I. (2025, September 3). ¿Qué es la seguridad de red? *Ibm.com*. https://www.ibm.com/mx-es/think/topics/network-security
- Flinders, M., & Smalley, I. (2025, September 3). ¿Qué es la seguridad de red? *Ibm.com*. https://www.ibm.com/mx-es/think/topics/network-security
- *Operating System Security*. (n.d.). Sciencedirect.com. Retrieved October 28, 2025, from https://www.sciencedirect.com/topics/computer-science/operating-system-security
- ¿Qué es la seguridad informática? (2024, July 18). *Ibm.com*. https://www.ibm.com/mx-es/think/topics/it-security