Universidad Nacional Autónoma de México

Facultad de Ingeniería

División de Ingeniería Eléctrica

Sistemas Operativos

Profesor(a): Gunnar Wolf
Semestre 2024-2

Investigación

Trabajo escrito

Riesgos de Ciberseguridad en los Sistemas Operativos

Integrantes
➢ Flores Melquiades Evelyn Jasmin - 319112186
➢ Vera Garmendia Miriam Marisol - 319239748

Grupo: __6___

Cd. Universitaria a 14 de mayo de 2024

Objetivos

- ❖ Presentar los riesgos de ciberseguridad que los sistemas operativos obsoletos o desactualizados presentan.
- ❖ Comprender la importancia de mantener actualizados los sistemas operativos que manejamos.
- ❖ Conocer acerca de los mejores sistemas operativos en términos de ciberseguridad y cuales son sus ventajas.

Introducción

¿Qué es un Sistema Operativo?

El *sistema operativo* es un conjunto de programas profesionales completamente integrado que gestiona todo el trabajo informático que permite monitorear y controlar la ejecución de todos los otros programas de la computadora como lo son la memoria, los discos, el almacenamiento de datos, la red y diferentes recursos de la computadora. Algunos ejemplos de sistemas operativos conocidos son Windows, Linux y Mac OS.

¿Qué es la ciberseguridad?

La *ciberseguridad* es la práctica de proteger sistemas, redes y programas de ataques digitales que buscan acceder, modificar o destruir información confidencial, extorsionar usuarios o interrumpir la continuidad del negocio. También se refiere a salvaguardar la información personal, cuentas, archivos y activos digitales, tanto a nivel personal como empresarial. Las organizaciones implementan medidas de ciberseguridad para mantener la confianza del cliente, cumplir con la normativa y evitar interrupciones en las operaciones. Esto implica optimizar la defensa digital a través de personas, procesos y tecnologías.

Desarrollo

Principales riesgos

- Falta de parches
  - Los sistemas operativos se encuentran en constante mantenimiento, con lo cual es posible identificar vulnerabilidades de seguridad que inicialmente no se conocían o no se habían abordado, siendo este el caso, las nuevas actualizaciones contienen los parches que cubren esas irregularidades encontradas.
  - Los sistemas operativos obsoletos o bien, que han superado cierto periodo de soporte, no reciben este tipo de actualizaciones por lo que es mas sencillo que esas vulnerabilidades se vean mas expuestas a personas que se dedican a explotar información sensible, y siendo mas susceptible a amenazas emergentes.

- Ausencia de actualizaciones de seguridad
  - Pérdida de datos
  - Reducción de productividad
  - Defensa obsoleta e ineficaz frente a nuevas amenazas
  - Los sistemas operativos más recientes pueden tener mejores algoritmos de cifrado que no están disponibles en los sistemas antiguos, y al no tener estas actualizaciones los hace menos resistentes a ataques como el robo de datos.
- Problemas de incompatibilidad
  - Dificultad para integrarse con nuevas aplicaciones y hardware con el paso del tiempo
  - Complica la implementación de funciones avanzadas.
- Soporte limitado
  - Al ser una versión antigua del sistema, el recibir asistencia del proveedor se convierte en un problema, dado que ellos se centran en la línea de producto actual e incluso futura.
  - Se da lugar a largas interrupciones durante las crisis del sistema o de seguridad.
    - Por ejemplo, Microsoft ya no da soporte a Windows 7 ni a versiones anteriores
    - Apple ya no da soporte a versiones de macOS anteriores a macOS 11 (Big Sur).
    - Algunas versiones de distribuciones de Linux llegan a tener diferentes ciclos de vida de soporte,dependiendo de la comunidad o la empresa que las respalda.
- Incumplimiento de normas
  - Las organizaciones industriales a menudo tienen que cumplir estrictos criterios de conformidad que exigen el uso de sistemas actualizados y seguros. Utilizar un sistema operativo obsoleto puede dar lugar a incumplimientos, multas y daños a la reputación de la organización.

Tipos de riesgos

- Malware
  - Programas maliciosos pueden dañar sistemas, robar información o permitir el acceso no autorizado a dispositivos; algunos ejemplos son los virus, bugs, troyanos y spyware.
- Phishing
  - Una manera de engañar a la gente para que ésta revele información confidencial, como contraseñas o datos financieros, a menudo a través de correos electrónicos o sitios web falsos.
- Ransomware
  - Cifran los archivos de las víctimas y amenazan con mantener bloqueados sus datos, a menos que la víctima pague un rescate al atacante.

- Ataques de denegación de servicio (DDoS)
    - Inundan los servidores o redes con tráfico falso, provocando la caída de los sistemas y servicios. Interrumpen el funcionamiento normal de una empresa u organización.
- Ataques de fuerza bruta
    - Intenta adivinar contraseñas o claves de cifrado probando todas las combinaciones posibles de forma sistemática y repetitiva hasta encontrar la correcta.
- Ataques avanzados persistentes (APT)
    - Los atacantes pueden infiltrarse en redes y sistemas durante meses o años sin ser detectados lo cual puede llegar a ser potencialmente destructivo.

Consecuencias negativas de una ciberseguridad deficiente

- Pérdida de datos
- Fuga de información
- Acceso no autorizado
- Fuga de contraseñas

Estrategias para prevenir riesgos

- Evaluar riesgos
    - Identificar todos los sistemas viejos de la organización y evalúe su importancia, con lo que es mas fácil determinar cual es mas factible actualizar.
- Aislamiento
    - Aislar los sistemas viejos del resto de la red en la medida de lo posible, realizando las medidas necesarias para minimizar la exposición a posibles amenazas.
- Supervisión de manera regular
    - Supervisar de manera continua los sistemas viejos para detectar anomalías o brechas.
- Virtualización
    - Virtualizar los sistemas heredados, lo cual aumenta el nivel de aislamiento y seguridad mientras permite ejecutar aplicaciones actualizadas en un sistema más reciente.

Ejemplos de ataques

- Ransomware WannaCry
    - En el año 2017, este ataque explotó una vulnerabilidad en el sistema operativo Windows que fue parcheada por Microsoft, sin embargo una gran cantidad de organizaciones no habían instalado dicha actualización; provocando que este ataque se propagara alrededor del mundo e infectara miles de sistemas llevando consigo una gran pérdida financiera.

- Fallo Heartbleed
  - Fue una vulnerabilidad en la biblioteca de cifrado OpenSSL la cual afectaba a sistemas operativos como Linux y Windows. Al ejecutarse versiones obsoletas de OpenSSL en estos sistemas, dejaba expuesta información confidencial(contraseñas o claves de cifrado).
- Vulnerabilidad de Apache Struts
  - En 2017, debido a una vulnerabilidad en el framework web Apache Struts la cual ejecutaba una version obselata; Equifax sufrió una violación masiva de datos, la cual expuso información personal de millones de clientes. Cabe aclarar que esta vulnerabilidad había sido parcheada, sin embargo la empresa no actualizó su sistema.
- Bug Stuxnet
  - En las versiones obsoletas de Windows, se dio lugar a un ataque de malware dirigido a sistemas de control industrial, el cual estaba principalmente diseñado para interrumpir el programa nuclear iraní. Provocó daños físicos a centrifugadoras y otras infraestructuras críticas.
- Bot Mirai
  - Un ataque masivo de denegación de servicio distribuido (DDoS) en 2016; dirigido a un proveedor de servicios de nombres de dominio el cual logró derribar web populares como Twitter y Netflix. Esto se debió a una vulnerabilidad del firmware y los sistemas operativos obsoletos.

Sistemas Operativos con mejor ciberseguridad

1. Linux
2. Kali Linux
3. Parrot Security
4. BackBox Linux
5. BlackArch Linux

Conclusiones

La gestión de los sistemas operativos exige tener un minucioso equilibrio entre la conservación de funciones cruciales y la resolución de los problemas de ciberseguridad con los que se asocian. Se tiene entendido que las organizaciones deben ser conscientes de los riesgos potenciales de los sistemas operativos viejos y adoptar nuevas estrategias para proteger y, con el tiempo, sustituir estos sistemas obsoletos. Hoy en día las ciberamenazas se fijan mas en las vulnerabilidades de los sistemas no actualizados, lo cual es necesario tener un enfoque en la gestión de riesgos y tenerlos en cuenta nosotros como usuarios.

Referencias

- *5 Outdated Software Risks and How You Can Find and Fix Them*. (s. f.). Bitsight. https://www.bitsight.com/blog/outdated-software-issues

- *Anatomía de un ataque*. (2024, 23 febrero). [Vídeo]. Cisco. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
- *Conoce cuáles son las principales herramientas de Ciberseguridad a seguir durante este 2021*. (s. f.). KIO. https://www.kio.tech/blog/conoce-cu%C3%A1les-son-las-principales-herramientas-de-ciberseguridad-a-seguir-durante-este-2021#:~:text=Kali%20Linux%20es%20conocido%20como,para%20la%20auditor%C3%ADa%20de%20seguridad
- Convergence, I. (2024, 20 febrero). *Risks of Using Outdated Operating System*. IT Convergence. https://www.itconvergence.com/blog/risks-of-using-outdated-operating-system/
- Formación, A. (2023, 29 noviembre). *Tipos de riesgos en Ciberseguridad*. ADR Formación. https://www.adrformacion.com/knowledge/internet/tipos_de_riesgos_en_ciberseguridad.html
- Laprovittera, C. (2023, 7 diciembre). *Los 10 Mejores Sistemas Operativos para Pentesting y Ethical Hacking en 2024*. Álvaro Chirou. https://achirou.com/los-10-mejores-sistemas-operativos-para-pentesting-y-ethical-hacking-en-2024/
- Milestone. (2024, 14 mayo). *Legacy Operating Systems and the Cybersecurity Risks they Carry*. Milestone Technologies - IT Services And Digital Solutions. https://milestone.tech/uncategorized/legacy-operating-systems-and-the-cybersecurity-risks-they-carry/
- *¿Qué es la ciberseguridad? - Soporte técnico de Microsoft*. (s. f.). https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390
- *Riesgos de ciberseguridad por utilizar un sistema desactualizado*. (s. f.). https://blog.cobistopaz.com/es/blog/riesgos-de-ciberseguridad-por-usar-sistemas-desactualizados