Actividad 1 – Análisis de Vulnerabilidades y Amenazas

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Kathya Viridiana Chávez Domínguez

Fecha: 28/04/2024

Índice

Introducción

La seguridad informática es una rama de la seguridad que le permite a las organizaciones proteger los sistemas informáticos, redes y dispositivos digitales de amenazas tanto externas como internas. Su alcance es amplio y requiere la implementación coordinada de tecnologías y soluciones de seguridad que trabajan en conjunto para identificar y reducir las vulnerabilidades e una organización.

A través de esta actividad, abordaremos a detalle el concepto, la importancia y el uso de la seguridad informática. Además, analizaremos un caso de estudio centrado en un colegio educativo para poder analizar los diferentes factores con los que trabajan y así lograr identificar sus posibles fuentes de amenazas y vulnerabilidades. Al finalizar, nuestro objetivo es comprender mejor el papel crítico que desempeña la seguridad informática en las empresas de hoy en día, sobre todo considerando el constante avance tecnológico. Así mismo, obtendremos la habilidad de identificar y prevenir amenazas en nuestro trabajo actual o en futuros proyectos.

.

Descripción

En esta ocasión, se busca implementar medidas de seguridad informática en un colegio de educación superior. Para lograrlo, se llevará a cabo un análisis detallado de los siguientes factores, clasificando las vulnerabilidades y amenazas identificadas.

Escenario principal:

- La institución educativa se encuentra en Veracruz , cerca de la costa.
- Su infraestructura es de 2 pisos con 18 salones , 3 departamentos (Contabilidad y finanzas / Dirección / Desarrollo Académico/ , así como un centro de cómputo y una biblioteca.
- Actualmente tiene 4 escaleras de acceso a planta superior y 1 ascensor principal.
- Presenta una entrada principal 2 laterales y posterior a la cancha principal una salida.
- Los docentes registran su entrada en una libreta y los departamentos utilizan tarjetas de registro .
- El área administrativa financiera no cuenta con una alarma de seguridad para su acceso.
- Se cuenta con 2 extintores Clase A y uno Clase B ubicados en el piso principal.
- Se cuenta con una salida de emergencia.
- No se identifica dispositivo de detección de sismos, u otros fenómenos naturales.
- Se cuenta con un servidor principal(diferente al del centro de cómputo).

El centro de cómputo presenta la siguiente infraestructura:

- 1 Servicio de internet de 20GB comercial.
- 10 equipos de escritorio.

- 5 laptops.
- 1 servidor espejo.

En los departamentos se presenta la siguiente infraestructura:

- 4 equipos por departamento.
- Los equipos de la planta baja se encuentran conectados por cable de manera directa al módem. Los del piso de arriba son portátiles y se conectan vía wifi.
- Los equipos han estado lentos en el último mes y se están quedando sin espacio de almacenamiento.

Detalles adicionales:

- Cada equipo cuenta con un usuario y contraseña básicos, por ejemplo:
- Usuario: Equipo1
- Password: 1234abc
- El firewall no se encuentra habilitado.
- El antivirus es nod32 versión gratuita en todos los equipos.
- No se tiene denegado el uso del equipo para actividades personales, por ejemplo, el acceso a redes sociales o el manejo del correo electrónico o WhatsApp.
- El Servidor cuenta con la base de datos general. Este utiliza el software Oracle Database en un sistema operativo Linux. Por su parte, el Servidor 2 se destina para alojar un sistema de control que descargaron de Internet, y que les ayuda para mantener los registros de los alumnos (se desconoce la fuente de este software)

Para esta actividad se debe de tomar en cuenta el escenario presentado para analizar y realizar una tabla de las posibles fuentes de amenazas y vulnerabilidades, contemplando las amenazas

humanas, lógicas y físicas. Así como las vulnerabilidades de almacenamiento y de comunicación.

Justificación

Tomando en cuenta el avance de la tecnología, la sensibilidad hacia la seguridad informática ha aumentado significativamente. Por lo que garantizar un acceso y uso seguro de la información almacenada en diferentes dispositivos, así como protegerse contra posible ataques y amenazas mediante el análisis de vulnerabilidades y amenazas, se ha vuelto fundamental para cualquier organización. Esto es muy importante considerando las graves implicaciones y costos asociados a las fallas de seguridad de datos que pueden ir desde la pérdida de empleo hasta la pérdida de ingresos e imagen empresarial. Así mismo se vuelve fundamental pensar en la protección de datos y establecer defensas desde el inicio del proceso. Por esta razón, la seguridad informática implementa diferentes mecanismos para abordar y solucionar cualquier problema que se pueda presentar en los sistemas informáticos, ya sea debido al uso inadecuado por parte de los usuarios internos o ante posibles ataques efectuados por hackers y ciberdelincuentes, quienes buscan aprovechar alguna vulnerabilidad para acceder a los sistemas y datos sensibles de las organizaciones y sus usuarios.

Desarrollo

Tabla de Análisis

Amenazas Humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de Comunicación
Acceso no vigilado en el área administrativa: El área administrativa del colegio es altamente sensible debido a la naturaleza de los datos que almacena. Por desgracia, actualmente carece de sistemas de alarma de seguridad al acceder, lo que podría permitir el acceso no autorizado y la potencial obtención de información confidencial para fines no autorizados.	**Riesgos de red:** La ubicación del servidor principal fuera del centro de cómputo implica la necesidad de mantener conexiones de red adicionales. Esto expande la superficie de ataque de la red, convirtiendo cada nueva conexión en un posible punto de entrada para un atacante.	**Huracanes:** Tomando en cuenta la ubicación de Veracruz, una de las amenazas físicas a las que se está expuesto son los huracanes, los cuales pueden causar vientos, lluvias e inundaciones lo que puede resultar en daños materiales y afectaciones a las infraestructuras. Esto es muy grave, sobre todo considerando que el colegio carece de un dispositivo de detección de eventos naturales, lo que aumenta la vulnerabilidad de los equipos ante tales eventualidades.	**Registro de entrada:** El registro de la entrada de los docentes en una libreta puede parecer una tarea simple, pero en realidad conlleva una vulnerabilidad significativa. Existe el riesgo de pérdida de la libreta, lo que implicaría la pérdida de la información registrada. Además, recuperar datos de meses o años anteriores puede resultar difícil, especialmente si la libreta se llenó en algún momento y fue reemplazada por otra.	**Servidor principal puede ocasionar problemas de comunicación y rendimiento:** La calidad de la conexión entre el servidor principal y el centro de cómputo debe ser óptima, ya que de lo contrario podría generar problemas de comunicación o rendimiento. Esto afectaría la accesibilidad y la eficiencia de los servicios ofrecidos.
Ataques dirigidos: Tomando en	**Seguridad de la red Wi-Fi:** Dado que	**Deslizamientos de tierra:** Dada la presencia de	**Riesgo de pérdida de datos:** Debido a	**Interferencias y señales débiles:** Los

cuenta que solo disponemos de una salida de emergencia, existe el riesgo de que un posible atacante concentre sus esfuerzos en identificar y explotar esta única vía. Esto podría lograrse mediante ataques de denegación de servicio u otras técnicas que comprometan o interrumpan el sistema, dejando vulnerables a quienes dependen de ella en situaciones críticas.	contamos con dispositivos portátiles que se conectan a través de Wi-Fi, la seguridad de esta conexión se ve comprometida. Este tipo de conexión es más susceptible a ser interceptada o comprometida en comparación con las conexiones por cable, ya que los atacantes podrían intentar acceder a la red mediante técnicas como la suplantación de identidad y el descifrado de contraseñas débiles.	zonas montañosas en Veracruz, las fuertes lluvias pueden desencadenar deslizamientos de tierra, representando un riesgo para los equipos, especialmente aquellos ubicados en la planta baja que están conectados directamente al módem a través de cables.	la falta de almacenamiento en los equipos, es más probable que ocurran errores al guardar los datos, lo que podría resultar en la pérdida de archivos importantes. Esto comprometería la disponibilidad de información sensible para el colegio.	equipos portátiles que se conectan a través de Wi-Fi pueden experimentar interferencias y alcances limitados, especialmente al considerar su ubicación en un segundo piso. Esto puede traducirse en conexiones inestables y problemas de rendimiento.
Acceso físico a la información facilitado: Los dispositivos portátiles son más susceptibles al acceso físico no autorizado, especialmente si se permite que sean transportados fuera del lugar de trabajo. Esto aumenta el riesgo de robo de datos, incluso por parte	**Riesgo de malware y ataques:** Los equipos con bajo espacio de almacenamiento y rendimiento lento son más propensos a infecciones por malware y ataques cibernéticos. Esta vulnerabilidad se incrementa especialmente	**Tipo de extintores disponibles:** Actualmente, contamos con dos extintores Clase A y uno Clase B ubicados en el piso principal. Sin embargo, considerando que nuestras instalaciones abarcan dos pisos, 18 salones, el	**Diferencia en los datos almacenados:** Si el servidor espejo ubicado en el centro de cómputo no está configurado correctamente con el servidor principal, podrían surgir diferencias en los datos. Esto podría ocasionar inconsistencias en la información o	**Ataques de denegación de servicio (DDoS):** La presencia de un servidor espejo aumenta la probabilidad a un ataque DDoS, el cual sobrecarga los recursos de red y agota la capacidad de procesamiento. Este tipo de ataque podría

de los propios empleados, sobre todo si no se implementan las medidas de seguridad adecuadas.	cuando los usuarios descargan e instalan software, parches de seguridad y actualizaciones sin precaución, lo que aumenta la probabilidad de instalar malware o software no autorizado.	centro de cómputo y la biblioteca, varias áreas quedan desprotegidas en caso de un incendio. Es importante destacar que los extintores disponibles son eficaces para combatir incendios que involucran materiales combustibles comunes, como madera, papel, tela y plástico (tipo A), así como para extinguir incendios que implican líquidos inflamables o combustibles (tipo B). Sin embargo, esta selección de extintores no garantiza la protección adecuada de los dispositivos electrónicos, ya que no incluye el extintor de dióxido de carbono (tipo C). Este último es crucial, ya que no deja residuos y no	incluso pérdida de datos.	provocar una interrupción del servicio para los usuarios.

		conduce electricidad, lo que lo hace seguro para su uso en entornos con equipos electrónicos. Su ausencia podría representar un riesgo para la integridad de nuestros dispositivos en caso de un incendio.		
Exposición a las amenazas internas: Los dispositivos con bajo rendimiento y poco espacio de almacenamiento pueden ser objeto de abuso por parte de empleados malintencionados. Estos dispositivos ofrecen una mayor oportunidad para el robo de datos confidenciales o la realización de actividades no autorizadas, aprovechando la falta de controles y la lentitud del sistema.	**Ataques de autenticación:** Dado que los equipos utilizan credenciales de usuario y contraseña básicas, se vuelven vulnerables a los ataques de autenticación, tales como el Spoofing-Looping, el Ip Splicing-Hijacking y el Net Flooding.	**Punto único de fallo:** Depender únicamente de una sola salida de emergencia nos expone a un punto crítico. Si esta salida llegara a fallar o ser comprometida de alguna manera, toda la infraestructura o sistema podría volverse inaccesible.	**Fuga de información sensible:** La falta de un firewall puede ocasionar la salida no autorizada de datos sensibles de la organización, comprometiendo la confidencialidad de la información.	**Riesgo de sobrecarga en la red:** Considerando que el centro de cómputo cuenta con 10 equipos de escritorio, 5 laptops y 1 servidor espejo, depender de un servicio de internet con una capacidad limitada de 20 GB podría provocar una sobrecarga de red si no es capaz de soportar el tráfico generado por todos los dispositivos. Esto podría afectar la disponibilidad y el rendimiento de los servicios..

Exposición a amenazas externas: Tomando en cuenta que en los equipos no se tiene denegado el acceso a redes sociales, correo personal o WhatsApp, los empleados pueden exponerse a amenazas externas, como perfiles falsos, ataques de ingeniería social o intentos de robo de identidad.	**Menor capacidad de detección a malware y limpieza:** Debido a que se utiliza la versión gratuita del antivirus nod32 en todos los equipos, su capacidad de detección y limpieza es inferior en comparación con las versiones comerciales. Esto puede resultar en una menor eficacia para detectar y eliminar malware, aumentando así el riesgo de infecciones y compromisos de seguridad.	**Servidor principal propenso a las amenazas físicas:** El servidor principal está expuesto a diversas amenazas físicas debido a su ubicación fuera del centro de cómputo principal. Riesgos como desastres naturales, incendios, robos o daños accidentales pueden provocar la pérdida de datos o la interrupción del servicio.	**Vulnerabilidades de Oracle Database:** Contemplando que el servidor utiliza el software Oracle Database en un sistema operativo Linux, es importante considerar que puede contener vulnerabilidades de seguridad propias, como errores de programación e inyecciones de SQL. Estas vulnerabilidades podrían ser explotadas por atacantes para acceder o manipular los datos almacenados en la base de datos.	**Ataques de red:** La ausencia de un firewall habilitado expone nuestros sistemas a ataques que pueden agotar los recursos del sistema y causar interrupciones en los servicios.
	Malware y software malicioso: Dado que el Servidor 2 aloja un sistema de control descargado de internet, cuya fuente y origen		**Fuga de datos y violaciones de privacidad:** La utilización de software de origen desconocido en el Servidor 2 podría ocasionar fugas de datos o	

	son desconocidos, existe el riesgo de que contenga malware como virus, troyanos o ransomware. Esto podría comprometer la seguridad del servidor y poner en riesgo la integridad de los datos almacenados.		violaciones de privacidad. Esto puede ocurrir si el software recopila, almacena o transmite información de los alumnos sin el consentimiento adecuado.	

Conclusión

A través de esta actividad, hemos tenido la oportunidad de analizar y reconocer diferentes amenazas y vulnerabilidades que se podrían dar en un colegio de educación, según el escenario y los detalles presentados. Esta experiencia nos ha brindado una perspectiva más amplia sobre la importancia del análisis en seguridad informática para los dispositivos y formas de trabajar que podrían surgir.

Es importante tomar en cuenta que cada detalle pasado por alto puede traer consigo diferentes situaciones que comprometan la integridad de la información y los datos utilizados, desde problemas de almacenamiento hasta ataques cibernéticos por parte de hackers o personal interno. Al identificar estas posibles amenazas y vulnerabilidades estamos mejor preparados para tomar decisiones informadas con la finalidad de fortalecer la seguridad de nuestra infraestructura tecnológica. Esto nos ayuda a mitigar los riesgos de posibles ataques y proteger tanto los datos de la organización como conseguir la confianza de sus usuarios. Sin duda, este conocimiento adquirido será fundamental en el transcurso de la carrera y sobre todo en futuros proyectos.

Link GitHub: https://github.com/KathyaCh/An-lisis-de-Vulnerabilidades-y-Amenazas.git

Referencias

I. Comunicación. (2022, 18 noviembre). *La Seguridad Informática y sus beneficios*. Ciencias del Derecho. https://cienciasdelderecho.com/seguridad-informatica-beneficios/

II. Martín, E. (2023, 8 junio). ¿Qué es la seguridad informática y cómo implementarla? *Cibernos Grupo*. https://www.grupocibernos.com/blog/que-es-la-seguridad-informatica-y-como-implementarla

III. Noguera, D. (2024, 1 marzo). *¿Son seguras las redes Wi-Fi? Descubre los riesgos y vulnerabilidades - FlashStart*. FlashStart. https://flashstart.com/es/son-seguras-las-redes-wifi-descubre-los-riesgos-y-vulnerabilidades/

IV. *¿Qué es la seguridad informática? | IBM*. (s. f.). https://www.ibm.com/mx-es/topics/it-security

V. *¿Qué es un ataque DDoS? | IBM*. (s. f.). https://www.ibm.com/mx-es/topics/ddos

VI. *Seguridad de datos: En qué consiste y qué es importante en tu empresa*. (s. f.). https://www.powerdata.es/seguridad-de-datos

VII. *Vulnerabilidades en Oracle*. (2020, 21 abril). https://www.entelgy.com/divisiones/innotec-security/actualidad-innotec-security/vulnerabilidades-innotec-security/vulnerabilidades/vulnerabilidades-en-oracle