

Actividad 2 - Prevención de fuentes de ataques e intrusión

Seguridad Informática 1

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Fernando Pedraza Garate

Fecha: 31 de Diciembre del 2023

Índice

Etapa 1 – Análisis de Vulnerabilidades y Amenazas

- Introducción. Pág. 3-4
- Descripción Pág. 5-6
- Justificación Pág. 7
- Desarrollo Pág. 8
 - Tabla de análisis

Etapa 2 – Prevención de fuentes de ataques e intrusión

- Justificación Pág. 9
- Desarrollo Pág. 10-13
 - Tabla de recomendaciones
- Conclusión Pág. 14
- Referencias Pág. 15-16

Introducción

Un análisis de riesgos y vulnerabilidades es un método para definir, identificar, clasificar y priorizar las debilidades de una aplicación, servicio, organización, etc., el realizar un análisis de riesgos y vulnerabilidades ayuda a proteger cualquier organización, sistema o proceso de posibles amenazas, identificando los riesgos más críticos y desarrollando un plan de mitigación de riesgos efectivo siguiendo los siguientes pasos para proteger los activos críticos:

1. Primero se debe **identificar los activos críticos** que deben protegerse. Esto podría incluir información confidencial, sistemas de tecnología, edificios y otros recursos físicos.
2. A continuación **identificar las amenazas potenciales**, en el análisis de riesgos y vulnerabilidades se debe identificar las amenazas potenciales a los activos críticos. Esto podría incluir amenazas físicas como incendios o inundaciones, amenazas cibernéticas como ataques de hackers, y amenazas internas como el robo por parte de empleados.
3. Se debe **evaluar la vulnerabilidad de cada activo crítico a cada amenaza identificada**, cuestionando, ¿Qué tan vulnerable es cada activo a cada una de ellas?
4. Se debe **evaluar el impacto potencial** de cada amenaza en cada activo crítico, cuestionando, ¿Qué tan grave sería el daño si se explotara una vulnerabilidad?
5. Se debe **Calcular el riesgo** para cada amenaza y activo crítico. El riesgo se calcula multiplicando la probabilidad de que ocurra una amenaza por el impacto potencial de esa amenaza.
6. Posteriormente **se deberán priorizar los riesgos**, identificados por su nivel de riesgo, dando prioridad a los riesgos más críticos.

7. También se deberá **desarrollar un plan de mitigación de riesgos** para abordar los riesgos más críticos, esto podría incluir la implementación de medidas de seguridad físicas o cibernéticas, la creación de políticas y procedimientos, y la capacitación del personal.
8. **Monitorear y actualizar** el plan de mitigación de riesgos regularmente para asegurarse de que se mantenga actualizado y efectivo.

Las medidas de ciber seguridad en aplicaciones web son importantes para proteger datos sensibles, prevenir ataques cibernéticos, mantener la integridad de las aplicaciones y cumplir con las regulaciones normativas.

Definición del contexto.

Se pretende aplicar mecanismos de seguridad informática a un colegio de educación superior ubicado 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, respecto al 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 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.

Otros detalles, 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, 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).

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, uno 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 y se cuenta con un servidor principal (diferente al del centro de cómputo).

De acuerdo al escenario presentado se deberá analizar y realizar una tabla de las posibles fuentes de amenazas y vulnerabilidades, por ejemplo:

(Amenazas: humanas, lógicas y físicas; Vulnerabilidades: almacenamiento y comunicación).

Posteriormente se deberán realizar las recomendaciones de seguridad en relación a los eventos identificados, planificando, mejorando e implementando las medidas necesarias para proteger tanto la parte física como la parte de la información, recordando y teniendo en cuenta que la información que no sea asegurada será un factor crítico para cualquier institución,

Justificación.

Se recomienda emplear este tipo de solución para poder concentrar toda la información necesaria de forma simple y entendible a través de un levantamiento general que incluya los pros y contras de todo el panorama existente, para así posteriormente, poder priorizar las actividades de acuerdo a los departamentos establecidos y poder mejorar la seguridad tanto de la red en general como de su infraestructura, auditando de forma sencilla el nivel de seguridad de cada parte de la misma y de los usuarios, atacando los focos rojos en primera instancia, logrando aislar la información de personas ajenas a esta, creando y otorgando perfiles de acceso a usuarios clave de acuerdo a sus perfiles dentro del organigrama establecido y si tendrán acceso al sistema o no, lo que permitirá identificar las fuentes de amenazas, ya sean humanas, lógicas o físicas y las vulnerabilidades existentes, como el almacenamiento y la comunicación, logrando cumplir con el objetivo de mantenimiento y mejora enfocada.

Desarrollo.

Tabla de análisis

Amenazas Humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de comunicación
Hacker	Software incorrecto	Incendios	Denegación DoS y DDoS	Información no disponible
Cracker	Puertas traseras	Terremotos	Robo	Información alterada
Phreaker	Bombas lógicas	Inundaciones		
Insider	Virus			
Piratería informática	Gusanos			
	Troyanos			

Justificación.

Una vez identificadas las áreas de oportunidad encontradas de vulnerabilidad, mejora e implementación, tanto en la parte lógica como en la infraestructura, como ya se mencionó con anterioridad, se recomienda sugerir al menos una recomendación sustentada para cada una de ellas y así poder proteger, mejorar y monitorear dichos eventos, priorizando los aspectos más importantes a los problemas identificados, dando relevancia en todo momento a la información como fuente principal de gran valor para cualquier negocio, empresa o compañía, para evitar daños irreparables, alteraciones o pérdidas de la misma, ya sea esto causado por un descuido interno, mala práctica de los responsables, robo de algún personal interno o la intrusión de algún atacante en la red, y en la parte física del mismo modo se deben sugerir los cambios necesarios para proteger los equipos de cualquier daño natural que no se pueda predecir con antelación, como son los terremotos, incendios, e inundaciones.

Desarrollo.

Tabla de recomendaciones			
	Factor de riesgo:	Recomendación:	Fuente de ataque e intrusión:
Amenazas Humanas:	Contraseña generalizada a todos los usuarios (1234abc)	Generar contraseña por usuario y más seguras, con fecha de caducidad para la creación de un nueva	Pone en riesgo las cuentas de usuarios a que se puedan hackear consciente e inconscientemente
	Vulneración al sistema de seguridad	Habilitación y configuración adecuada del firewall	Vulneración al sistema de seguridad por algún cracker por múltiples razones, ya sea por fines de lucro, protesta o desafío
	Phreaker, insider, pirateo informatico	Instalación y mantenimiento de un antivirus actualizado	Intercepción de la red

Amenazas Lógicas:	Versión de software antivirus gratuito	Obtener la versión Pro del antivirus para que cuente con todas las características de protección ofrecidas y recomendadas	Pone en riesgo todos los equipos y el sistema al estar limitado por ser una versión gratuita
	Puerta Trasera	Configurar y denegar el uso del equipo para actividades personales, por ejemplo, el acceso a redes sociales o el manejo del correo electrónico o whatsapp	Ataques por malware y spam ocasionados por no tener restricción de uso en los equipos de la institución
	Bombas Lógicas, virus, gusanos y troyanos	Evitar descargar archivos de enlaces o direcciones web sospechosas, configuración de privacidad de la red y del correo electrónico	Descarga de archivos infectados

Amenazas Físicas:	Incendio no controlado	Instalación de detectores de humo en todas las áreas y en el centro de cómputo adecuar el site de forma adecuada para proteger la información.	Pone en riesgo la integridad de las personas y que se generen incendios no controlados
	Terremotos e inundaciones inesperados	Instalación de sensores, alarmas sísmicas y la creación de un plan de evacuación.	Natural
Vulnerabilidades de almacenamiento:	Denegación DoS y DDoS	Contar con una solución de ciberseguridad que mantenga monitoreado el análisis continuo de archivos para prevenir y detectar amenazas que impacten en la información	Inactividad por sobrecarga dejando los sistemas de ciberseguridad fuera de línea

Vulnerabilidades de comunicación:	Información no disponible	Verificar la conectividad entre los equipos, comprobar la red eléctrica, revisar y configurar los parámetros de la red, verificar el comportamiento de los dispositivos de conexión y realizar pruebas de optimización	Falla de comunicación interna y externa
Vulnerabilidades de almacenamiento:	Robo de información	Creación de control de acceso biométrico para todos en la institución y un control de acceso autorizado para visitantes	Robo de información e infraestructura por un mal control de acceso
Vulnerabilidades de comunicación:	Información alterada	Creación de accesos a la información de acuerdo a perfiles establecidos	Alteración de datos por falta de configuración a la información

Conclusión.

En conclusión como ya se mencionó con anterioridad, es de suma importancia enlistar cómo está conformada la estructura física de las instalaciones, las instalaciones de red, y la estructura lógica del hardware y software utilizado, este tipo de acción permitirá poder tener un panorama exacto de la situación actual, donde también se podrá observar la cantidad de personas que hacen uso de los equipos, bajo qué criterios, quienes tienen acceso al sistema, el tipo de privacidad que existe en la transferencia de la misma, si hay controles de acceso a las áreas restringidas, si cuentan con algún tipo de respaldo físico o virtual de la información, identificando qué tipo de sistema de emergencia existe en caso de haber algún desastre natural o incendio, y así poder enlistar que se debe priorizar para poder proteger de forma adecuada y mejorar la seguridad e integridad de la información, así como los equipos y las personas mismas, creando un plan de contingencia que en caso de existir algún incidente natural la información se pueda proteger de forma adecuada sugiriendo mantener un hábitat adecuado para el servidor y los equipos correspondientes.

Enlace Github: <https://github.com/Chifer888/Segiuridad-Informatica-1.git>

Referencias

Gutierrez, E. (2023, 22 marzo). Descubre cómo hacer un análisis de riesgos en tus apps. *Codster*.

<https://codster.io/blog/como-realizar-analisis-de-riesgos-vulnerabilidades/>

Tipos de amenazas: humanas. (2017, 10 febrero). Seguridad Informática BRM.

<https://seguridadeinformaticabrm.wordpress.com/2017/02/10/tipos-de-amenazas-humanas/>

Tipos de amenazas: lógicas. (2017, 10 febrero). Seguridad Informática BRM.

<https://seguridadeinformaticabrm.wordpress.com/2017/02/08/tipos-de-amenazas-logicas/>

Tipos de amenazas: físicas. (2017, 8 febrero). Seguridad Informática BRM.

<https://seguridadeinformaticabrm.wordpress.com/2017/02/07/tipos-de-amenazas-fisicas/>

Amenazas de seguridad. (2017, 7 febrero). Seguridad Informática BRM.

<https://seguridadeinformaticabrm.wordpress.com/2017/02/03/amenazas-de-seguridad/>

<https://www.ikusi.com/mx/blog/como-prevenir-los-ataques-de-denegacion-de-servicio/>. (s. f.).

<https://www.ikusi.com>.

Electropreguntas. (2023, 5 febrero). *Fallas de comunicación comunes en redes y cómo solucionarlas*. <https://electropreguntas.com/fallas-de-comunicacion-comunes-en-redes-y-como-solucionarlas/>

Sánchez, L. O., & Sánchez, L. O. (2023, 1 octubre). *¿Qué es un ataque de puerta trasera? ejemplos y cómo prevenirlo*. NordVPN. <https://nordvpn.com/es/blog/ataque-de-puerta-trasera/>

MacKay, J. (2023, 14 abril). Riesgos de ciberseguridad: ¿Factores humanos o fallos humanos? | Riesgo de ciberseguridad. *MetaCompliance*. <https://www.metacompliance.com/es/blog/cyber-security-awareness/cyber-security-risk>

Niubox. (2021, 30 septiembre). *Mantén a salvo tus datos: cómo funciona, cómo prevenir y cómo detectar el phishing*. Niubox. <https://niubox.legal/manten-a-salvo-tus-datos-como funciona-como-prevenir-y-como-detectar-el-phishing/>