Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 2 – Prevención de fuentes de ataque e intrusión

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: José Domingo Reyes Arroyo

Fecha: 30 de diciembre de 2023

1 Índice

1 Introducción

Tomando en cuenta el comportamiento de los ciberataques de los últimos años, estos, cada día son más numerosos y más sofisticados, cada vez con tendencias a incrementar y mejorar para estar a la par de ataques a sistemas mucho mas seguros. Es por ello que para mantener la seguridad de la información las medidas de seguridad se han convertido en la prioridad de las empresas o entidades que dependen del internet al 100% entre los tipos de ataques mas comunes, encontramos: malware, virus, gusanos, troyanos, spyware, adware, ransomware, phishing, ddos, entre otros. Para entender mejor el termino de ataques informáticos, estos se pueden definir como un intento organizado e intencionado que busca aprovechar alguna vulnerabilidad o debilidad de los sistemas o de las redes informáticas el cual puede ser tanto en el software como el hardware, siempre buscando el beneficio económico o en ocasiones por simple anarquía, hoy en día no son solo estos los ataques a los que están expuestas las empresas o las personas, en la actualidad podemos estar expuestos a ataques personales como ingeniería social, colaboradores malintencionados, propagación de datos confidenciales, extravió o hurto de dispositivos personales, poco control en las empresas o dependencias.

2 Descripción

Basado en estas definiciones de ataques informáticos e intrusiones y considerando el caso de estudio de la actividad anterior, en el cual se trabajó en el caso de un colegio de educación superior, realizando un análisis de ciertos factores que presentaban vulnerabilidades y

amenazas. Para la presente actividad se desarrollara el papel de analista de seguridad donde se realizaran las recomendaciones para eliminar la vulnerabilidad o amenaza de los eventos descritos, para esto se realizara una planificación mejora o implementación para cada evento, esto será necesario para proteger tanto la parte física como la parte de la información, se realizara una tabla de recomendaciones en la cual se describirá brevemente una o varias recomendaciones que ayuden a eliminar o disminuir cualquier amenaza o vulnerabilidad que se pueda encontrar dentro del colegio de educación superior, con la finalidad de proteger y salvaguardar la integridad de la institución y sobre todo para proteger la información delicada que pudiera contener el colegio en sus sistemas y también mejorar la seguridad física de las instalaciones de la propia institución.

3 Justificación

Dado que la seguridad de la información y la integridad de las personas que trabajan y estudian en la institución es la principal prioridad de esta, es por ello de suma importancia que como analista de seguridad desarrollemos propuestas de mejora e implementación de sistemas de seguridad tanto físicos como informáticos que garanticen la seguridad de la información que maneja la institución y sobre todo garantice la integridad de las personas que trabajan o estudian dentro del colegio de educación superior. A través de los años y los estudios que se han realizado sobre algunas empresas o instituciones en las que se han presentado casos de vulnerabilidad o amenazas todo evento que se ha presentado la responsabilidad principal ha recaído en la inseguridad presentada en puntos estratégicos como

los accesos, tanto físicos como de sistemas informáticos (contraseñas seguras), el cifrado de la información, la seguridad en bases de datos, etc., tal es el caso que se presento en Equifax en 2017, en donde se afectó a más de 145 millones de personas y tuvo un costo de mas de 700 millones de dólares, con se observa la seguridad informática de una institución o empresa debe ser lo primordial ya que puede representar pérdidas económicas y afectar a miles de personas.

4 Desarrollo

Continuando con la tabla de análisis que se elaboró en la actividad anterior, con los puntos relevantes que se consideran con vulnerabilidades y/o amenazas, de los cuales se propondrá una mejora o implementación que ayude a la institución a disminuir o eliminar el riesgo o vulnerabilidad detectado con anterioridad:

4.1 Tabla de recomendaciones

A continuación, se presenta la tabla con las propuestas de mejora para cada uno de los puntos relevantes, esta tabla se inserta como imagen, pero se sube al repositorio de GitHub el archivo en Excel del cual se extrajo la imagen de la tabla:

Factores	Amenazas humana	Amenazas lógicas	Amenazas físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de comunicación	Planeación, mejora o implementación
Ubicación			Se encuentra en la ciudad de Veracruz cerca de la costa			se recomienda implementar un sistema de seguridad ante inundaciones, promover que los equipos de computo sean resguardados en el segundo piso.
Infraestructura	Tiene 3 departamentos, 1 centro de computo y 1 biblioteca		Cuenta con 2 pisos y 18 salones			cambiar la estructura de los departamentos, donde los servidores y equipos de computo de escritorio se ubiquen en el segundo piso y tener un área de resguardo para los equipos portátiles en el mismo piso por cuestiones de inundación
Movilidad			Tiene 4 escaleras y un ascensor			colocar letreros para rutas de evacuación en escaleras, ubicando la vía mas corta, para acceso a los salones recomendar el uso de la escalera mas cercana al aula para evitar el Axeso de flujo de estudiantes, el ascensor solo usarlo para personas discapacitadas o para cuando se transporta material pesado
Accesos al edificio	Presenta 1 entrada principal, 2 laterales y una salida posterior a la cancha principal					dejar solo un acceso a las instalaciones, el cual se sugiere la entrada principal en caso de contar con 2 turnos, proponer la salida posterior, mientras el acceso para el segundo turno se realiza por el acceso principal, registrando a toda persona que entra o sale del edificio, contratar seguridad para acceso principal y salida posterior.
Entrada/Salida de personal	Los docentes se registran en una libreta y los administrativos con tarjeta					implementar que todos los docentes y administrativos cuenten con tarjeta o se implemente acceso por huella o chip en tarjeta de identificación, esta implementación también permitiría que el acceso de los alumnos sea por este medio para tener mas control de la cantidad de personas que alberga.
Seguridad en áreas financieras	El área administrativa y financiera no cuentan con alarma de seguridad					instalar alarmas de seguridad para acceso, ya sea con huella o clave (panel digital) para las áreas de riesgo
seguridad ante contingencias			Cuenta con 2 extintores clase A y 1 clase B			contratar proveedor de extintores e hidrantes, quien hará una planeación de los extintores e hidrantes que sean requeridos para todo el edificio, es mucho mejor con proveedor ya que se encargan de toda la planeación y garantía de los equipos así como su recarga y mantenimiento cada año
Salidas de emergencia			Cuenta con 1 salida de emergencia			implementar punto de reunión, el cual sea intermedio entre la entrada y la salida del edificio, para que ambas puedan fungir como salidas de emergencia, incluir en el tablero de acceso por huella o chip, la consulta de emergencia de la población total dentro del edificio para poder hacer un conteo rápido y validar si alguien no se quedo atrapado dentro del inmueble.
dispositivos de alarma			No se tiene detectores de humo, movimiento, impacto, etc.			con el mismo proveedor de extintores e hidrantes se hace la instalación de este tipo de sensores y la planificación de los que se requieren, en cuestión de los acceso se recomienda un sensor por entrada o salida para monitorear en horario no laborales si hay accesos no permitidos.
Servidores físicos		solo tiene 1 servidor				se recomienda la instalación de otro servidor para la cantidad de información que se maneja, dejar 1 exclusivo para administrativos y otro para alumnos. Implementar la creación de una base de datos en cada servidor con la información de cada docente y alumno necesarios.
Servicio de internet					1 servicio de internet de 20 GB comercial	aumentar la capacidad del internet de comercial a empresarial para mejorar el servicio y la velocidad de transferencia.
Equipos de escritorio				Cuenta con 10 equipos de escritorio		determinar la necesidad de equipos de escritorio según la cantidad de personas que trabajan en cada departamento para asegurar que cada administrativo cuente con un equipo.
Laptops				cuenta con 5 laptop		adquirir un equipo portátil para cada docente, el cual pueda ser usado tanto dentro de la institución como fuera de ella para que cada uno de los docentes pueda tener la información de los alumnos en su equipo.
Servidor espejo				cuenta con 1 servidor espejo		eliminar el servidor espejo y en su lugar contratar un servidor en la nube para tener la información respaldada en caso de alguna situación de desastre natural.
Conexión de los equipos					en planta baja es con conexión directa al modem por cable y en planta alta Wi-Fi	eliminar la conexión directa al modem e implementar que todos los equipos se conecten a través de Wi-Fi instalando VPN para mejorar la seguridad de la información, instalar repetidores para facilitar que la señal sea la misma en cualquier punto del edificio.
Condición de los equipos				Equipos lentos y sin espacio de almacenamiento		depurar los equipos de ser posible reiniciarlos de fabrica, para instalar software de limpieza y antivirus actualizados a todos los equipos.
Seguridad de los equipos		Usuario y contraseña básicos (Equipo-1, 1234abc)				implementar un administrador de contraseñas para implementar un usuario por departamento y una contraseña que cumpla con los requisitos de seguridad establecidos, además de generar un usuario por cada docente dependiendo de la materia y de la misma manera generar una contraseña segura

5 Conclusión

Tomando en cuenta el análisis previo a las implementación, se puede considerar esta actividad como clave para desarrollar habilidades como analista de seguridad para detectar vulnerabilidades que puedan tener los sistemas de cualquier empresa, como ingenieros en desarrollo de software debemos estar a la par de la seguridad informática, ya que es un tema que sin duda alguna es relevante para cualquier área de la informática a la que se enfoque un ingeniero en desarrollo de software, cabe destacar que estas actividades que permiten atender temas de seguridad informática y física para cualquier situación que se pueda presentar son cruciales para el aprendizaje personal y ayudan a poder detectar cualquier situación de vulnerabilidad dentro de la empresa incluso permiten tener una visión mas amplia de cualquier situación que pueda atentar contra la seguridad personal, física y de cualquier sistema informático, hoy en día las hackers no se enfocan solamente en sistemas operativos vulnerables, se enfocan en encontrar cualquier error en cualquier sistema operativo sea o no sea seguro, la idea es encontrar cualquier falla en los sistemas y hay quienes las usan para mejorar los sistemas y ayudar a perfeccionar el sistema operativo, pero también hay personas que se dedican a crear afectaciones en pequeña gran escala, es por ello que debemos estar preparados para cualquier situación en cuanto al tema de seguridad se refiera.

6 Referencias

Legro, A. (2023, 29 diciembre). Ataques informáticos: causas y 12 tipos de ciberataques. *Win Empresas*. https://winempresas.pe/blog/ataques-informaticos-causas-y-12-tipos-de-ciberataques

What is Intrusion Prevention System? | VMware Glossary. (2023, 26 noviembre). VMware. https://www.vmware.com/es/topics/glossary/content/intrusion-prevention-system.html

Prevención y detección de intrusiones. (s. f.). https://www.fortra.com/es/soluciones/seguridad-informatica/infraestructura/deteccion-y-prevencion-de-intrusiones

Actividad subida al repositorio de GitHub: https://github.com/drcksug/Seguridad-Informatica-I