Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 2. Prevención de Fuentes de Ataques e Intrusión

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: José Luis Pacheco González

Fecha: 9 de septiembre de 2024

Índice

Introducción

En la presente actividad, se busca complementar el análisis inicial de amenazas y vulnerabilidades realizado en la actividad uno, añadiendo las fuentes de ataque e intrusión correspondientes a cada elemento identificado. En la primera actividad se identificaron una serie de amenazas humanas, lógicas y físicas, así como vulnerabilidades tanto en los sistemas de almacenamiento como en los de comunicación de una institución. Sin embargo, para obtener una visión más completa y robusta de los riesgos a los que está expuesta la organización, es fundamental vincular cada amenaza y vulnerabilidad con sus posibles fuentes de ataque.

Este enfoque permite no solo identificar las debilidades existentes, sino también comprender los posibles métodos que podrían ser utilizados por los atacantes para comprometer los sistemas y acceder a información sensible. Las fuentes de ataque pueden incluir desde métodos tradicionales, como el phishing y los ataques de fuerza bruta, hasta técnicas más avanzadas como la interceptación de redes Wi-Fi o los ataques de man-in-the-middle. Al añadir estas fuentes de intrusión, se logra una evaluación más detallada y específica, que facilita la implementación de medidas de mitigación adecuadas y eficaces, ayudando así a fortalecer la seguridad general de la organización y a proteger sus activos críticos frente a posibles amenazas.

Descripción

En la actividad 1, se realizó un análisis exhaustivo de las amenazas y vulnerabilidades a las que se enfrenta una universidad, abordando tanto aspectos físicos como lógicos. El papel del analista de seguridad consiste en proponer recomendaciones que permitan mitigar o eliminar estos riesgos, protegiendo así tanto la infraestructura física como la información crítica de la institución. La información es un activo clave y si no se gestiona adecuadamente, puede convertirse en un factor de riesgo crítico, comprometiendo la operación y la reputación de la universidad.

La actividad actual se centra en la necesidad de investigar y sustentar cada amenaza y vulnerabilidad identificada, y redactar recomendaciones específicas para proteger los sistemas y prevenir fuentes de ataque e intrusión. Estas medidas deben cubrir tanto la mejora de la seguridad física como la protección de la información digital, y podrían incluir acciones como la implementación de firewalls, la adopción de políticas de contraseñas más robustas, la instalación de software antivirus actualizado, o la capacitación del personal para prevenir ataques de ingeniería social. Al aplicar estas recomendaciones, se busca no solo mitigar las amenazas actuales, sino también mejorar el monitoreo continuo para anticipar posibles incidentes de seguridad.

Justificación

La necesidad crítica de proteger tanto la infraestructura física como la información digital de la universidad, considerando que las amenazas y vulnerabilidades identificadas en la actividad 1 representan riesgos significativos para la seguridad operativa y la reputación institucional. La información es un recurso clave que, si no se gestiona y protege adecuadamente, puede convertirse en un blanco fácil para ataques externos e internos, afectando la confidencialidad, integridad y disponibilidad de los datos.

La planificación y ejecución de medidas de seguridad efectivas es crucial para prevenir posibles incidentes de seguridad, como filtraciones de datos, ataques de ransomware, accesos no autorizados o incluso robos físicos. Al investigar y proponer recomendaciones específicas para cada amenaza y vulnerabilidad, se busca no solo reducir el riesgo, sino también crear un entorno más seguro y resiliente ante ataques. Estas medidas pueden abarcar desde la implementación de sistemas de detección y prevención de intrusiones hasta políticas de contraseñas más estrictas y el fortalecimiento del control de acceso físico.

Desarrollo

- **Tabla de recomendaciones**

Amenazas humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de Comunicación
Uso de contraseñas débiles y fáciles de adivinar como "1234abc".	Falta de firewall habilitado,la red interna está expuesta a posibles accesos no autorizados o ataques externos.	Acceso físico no autorizado, entradas y salidas no controladas permiten el acceso no autorizado a la institución	Uso de software de fuentes desconocidas descargado sin verificar puede contener malware o backdoors.	Acceso a internet sin restriccione, Uso de la red para actividades no relacionadas con el trabajo, exponiéndose a phishing y malware.
Recomendación: Crear una política de contraseñas que requiera obligatoriamente una combinación de letras mayúsculas, minúsculas, números y caracteres especiales, con una longitud mínima de 12 caracteres. Además de programar el cambio de contraseñas cada 90 días y autenticación en dos pasos.	**Recomendación:** Instalar y configurar un firewall que pueda monitoree y controlar el tráfico de red entrante y saliente. Así como actualizar regularmente las reglas del firewall para adaptarse a nuevas amenazas y realizar auditorías periódicas de su configuración.	**Recomendación:** Uso de controles de acceso físico, como tarjetas de identificación con acceso restringido a áreas sensibles,cámaras de vigilancia en puntos estratégicos y utilizar sistemas de alarma para detectar accesos no autorizados.	**Recomendación:** Establecer una política de software que solo permita la instalación de aplicaciones aprobadas,utilizar repositorios oficiales y verificar la integridad del software antes de su instalación.	**Recomendación:** Utilizar filtros de contenido web que bloqueen sitios potencialmente peligrosos. Utilizar soluciones de seguridad de correo electrónico para filtrar mensajes de phishing.
Fuente de ataque e intrusión: Phishing y ataques de fuerza bruta.	**Fuente de ataque e intrusión:** Escaneo de puertos y ataques de denegación de servicio (DoS)	**Fuente de ataque e intrusión:** Intrusos físicos o empleados descontentos con acceso no autorizado.	**Fuente de ataque e intrusión:** Software malicioso descargado de internet, como troyanos.	**Fuente de ataque e intrusión:** Phishing, malware o ransomware descargado de sitios web maliciosos.

Acceso no autorizado a equipos para actividades personales,como el uso de redes sociales.	Antivirus gratuito puede no ser efectivo contra nuevas amenazas.	Falta de alarma de seguridad en área financiera, corre peligro de robo físico de información sensible o equipo.	Equipos con falta de espacio de almacenamiento, aumenta el riesgo de pérdida de datos o corrupción de archivos debido a un manejo inadecuado del almacenamiento.	Falta de protección de red en equipos conectados vía Wi-Fi y posible intercepción de datos.
Recomendación: Crear una políticas para límitar el uso de equipos institucionales para actividades personales. De igual manera utilizar un software de monitoreo que detecte y limite el acceso a sitios web no autorizados.	**Recomendación:** Actualizar a una solución antivirus comercial que ofrezca protección avanzada contra malware, ransomware y otras amenazas. Asegurarse de que todas las estaciones de trabajo y servidores tengan el antivirus instalado y actualizado regularmente.	**Recomendación:** Instalar sistemas de alarma en áreas críticas como la financiera. Implementar controles de acceso adicionales y monitoreo constante mediante cámaras de seguridad para detectar actividades sospechosas.	**Recomendación:** Expandir la capacidad de almacenamiento mediante la adquisición de SSD o soluciones de almacenamiento en la nube y realizar limpieza de datos para eliminar información innecesaria con la finalidad de liberar esacio.	**Recomendación:** Asegurar que la red Wi-Fi utilice protocolos de cifrado fuertes como WPA3 y utilizar autenticación segura para el acceso a la red. Tambien es recomendable segmentar la red para separar el tráfico administrativo del tráfico de invitados.
Fuente de ataque intrusión: Infección de malware o ransomware al descargar archivos o abrir enlaces maliciosos.	**Fuente de ataque intrusión:** Ataques de malware o ransomware que aprovechan antivirus desactualizados.	**Fuente de ataque intrusión:** Robo físico de dispositivos o documentos confidenciales.	**Fuente de ataque intrusión:** Corrupción de datos o acceso no autorizado debido a un sistema sobrecargado o lentitud en el procesamiento.	**Fuente de ataque intrusión:** Ataques de red (intercepción de datos, ataque de intermediario "man-in-the-middle").

Falta de concientización entre los empleados sobre buenas prácticas de seguridad.	Servidor espejo vulnerable en la misma red, se expone a ataques de red que pueden comprometer ambos servidores.	Ausencia de dispositivos de detección de sismos y otros desastres naturales que podrían dañar físicamente la infraestructura.	Contraseñas débiles almacenadas en equipos, fácilmente accesibles o predecibles, comprometen la seguridad de los datos almacenados.	Exposición a ataques de red por no tener firewall habilitado, debido a la falta de control de tráfico y filtrado de paquetes.
Recomendación: Realizar campañas de capacitación en seguridad informática cada determinado tiempo.Tambien es importante realizar simulaciones de phishing para entrenar a los empleados ante estos casos.	**Recomendación:** Segmentar la red para aislar el servidor espejo del servidor principal. Implementar controles de acceso estrictos y monitorear el tráfico entre los servidores para detectar actividades sospechosas.	**Recomendación:** Instalar sistemas de detección de sismos y otros dispositivos de alerta temprana, para asegurar que la infraestructura física esté reforzada para resistir desastres naturales.Realizar simulacros periódicos de evacuación y respuesta ante emergencias.	**Recomendación:** Utilizar gestores de contraseñas para almacenar credenciales de manera segura.	**Recomendación**: Además de habilitar el firewall, configurar reglas específicas para bloquear puertos innecesarios y monitorear el tráfico de red en busca de anomalías. Utilizar sistemas de detección y prevención de intrusiones (IDS/IPS) para reforzar la seguridad de la red.
Fuente de ataque e intrusión: Ingeniería social o phishing, donde los empleados son manipulados para entregar credenciales.	**Fuente de ataque e intrusión:** Ataques de "lateral movement" que aprovechan la falta de segmentación de red.	**Fuente de ataque e intrusión:** Daño físico a la infraestructura por fenómenos naturales.	**Fuente de ataque e intrusión:** Ataques de fuerza bruta o credenciales robadas debido a contraseñas débiles.	**Fuente de ataque e intrusión:** Ataques de red, incluidos escaneos de puertos y accesos no autorizados desde fuera de la red.

Uso inadecuado de recursos institucionales software y hardware. Provoca riesgo de introducir malware.	Sin restricciones en el uso de internet, genera riesgo de infecciones por malware debido a la navegación en sitios no seguros.	Extintores insuficientes en caso de incendio,riesgo de daño físico a equipos y pérdida de datos por fuego.	Lentitud en equipos debido a software no optimizado,afectación al rendimiento y aumento de la exposición a fallos de seguridad.	Riesgo de interceptación de comunicaciones por falta de cifrado,posibilidad de que datos sensibles sean interceptados y robados durante la transmisión.
Recomendación: Utilizar soluciones de gestión de dispositivos que limiten la instalación de software no autorizado y monitoreen el uso de hardware para detectar actividades inusuales.	**Recomendación:** Además de los filtros de contenido, implementar una red privada virtual (VPN) para asegurar las conexiones y utilizar soluciones de sandboxing para aislar actividades de navegación potencialmente peligrosas.	**Recomendación:** Aumentar la cantidad de extintores y asegurarse de que estén adecuadamente distribuidos en todas las áreas críticas. Se deben realizar inspecciones periódicas para garantizar que estén en buen estado y sean accesibles en caso de emergencia.	**Recomendación:** Optimizar el software mediante actualizaciones regulares y limpieza de archivos temporales. Considerar la actualización de hardware si es necesario para mejorar el rendimiento. Implementar herramientas de monitoreo de rendimiento para identificar y resolver cuellos de botella.	**Recomendación:** Implementar protocolos de cifrado fuertes (como TLS) para todas las comunicaciones de red. Utilizar VPNs para proteger las comunicaciones externas y asegurarse de que todas las aplicaciones que manejan datos sensibles utilicen cifrado de extremo a extremo.
Fuente de ataque e instrusión: Introducción de malware o spyware a través de software no autorizado.	**Fuente de ataque e instrusión**: Fuego que daña equipos y pérdida de información crítica almacenada.	**Fuente de ataque e instrusión**: Infección por malware a través de sitios web maliciosos.	**Fuente de ataque e instrusión**: Posibilidad de que los equipos colapsen y queden vulnerables a fallos de seguridad.	**Fuente de ataque e instrusión**: Ataques de "sniffing" de red y de "man-in-the-middle" que interceptan datos sensibles en tránsito.

Conclusión

La identificación y análisis de amenazas y vulnerabilidades en la universidad revelan importantes riesgos que comprometen tanto la seguridad física como la digital de la institución. El papel del analista de seguridad es esencial para mitigar estos riesgos mediante la implementación de medidas correctivas y preventivas, con el fin de proteger los activos más críticos, en especial la información sensible. La planificación adecuada y la aplicación de soluciones técnicas y operativas, como la mejora de contraseñas, la actualización de sistemas de protección llámese firewalls o antivirus, y la capacitación del personal para evitar ataques de ingeniería social, son pasos fundamentales para garantizar la seguridad.

Asimismo, es importante implementar sistemas de monitoreo continuo y fortalecer las políticas de acceso y control, tanto a nivel de infraestructura como de red. Al abordar cada amenaza y vulnerabilidad con recomendaciones sustentadas, se refuerza la seguridad de la institución frente a potenciales intrusiones o incidentes de seguridad.

La seguridad informática no es un proceso estático, sino dinámico, que requiere constante revisión y mejora. Por ello, las recomendaciones propuestas en esta actividad permiten no solo mitigar los riesgos actuales, sino también anticiparse a futuras amenazas, garantizando así un entorno más seguro y protegido para la universidad, su personal y sus estudiantes.

Referencias

Oficina de Seguridad del Internauta. (2017, marzo 8). ¿Cuáles son las amenazas más comunes en internet? Oficina de Seguridad del Internauta. https://www.osi.es/es/actualidad/blog/2017/03/cuales-son-las-amenazas-mas-comunes-en-internet

Enlace Github