Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |2| Prevención de fuentes de ataques e intrusos.

Seguridad Informática 1.

Ingeniería en Desarrollo de Sofwtare.

academiaglobal

TUTOR: Jessica Hernández Romero.

ALUMNO: Carlos Ariel Nicolini

FECHA: 06/01/2025

Índice

Introducción

Para prevenir ataques e intrusiones, se puede usar un sistema de prevención de intrusiones (IPS). En gran medida automatizadas, las soluciones de IPS ayudan a filtrar la actividad maliciosa antes de que llegue a otros dispositivos o controles de seguridad. Esto reduce el esfuerzo manual de los equipos de seguridad y permite que otros productos de seguridad actúen con mayor eficacia.

Las soluciones de IPS también son muy eficaces para detectar y prevenir la explotación de vulnerabilidades. Cuando se descubre una vulnerabilidad, suele haber una ventana de oportunidad para explorarla antes de que pueda aplicarse un parche de seguridad. Aquí se utiliza un sistema de prevención de intrusiones para bloquear rápidamente este tipo de ataques.

Los dispositivos de IPS se desarrollaron y lanzaron originalmente como dispositivos independientes a mediados de la década del 2000. Esta funcionalidad se ha integrado en soluciones de gestión unificada de amenazas (UTM), así como en los firewall de nueva generación. Las soluciones de IPS de nueva generación están ahora conectadas a servicios informativos y de red basados en la nube.

Existen varios tipos de soluciones IPS, que pueden implementar para diferentes fines. Estas incluyen:

- Sistema de prevención de intrusiones basado en la red (NIPS).
- Sistema de prevención de intrusiones en host (HIPS).
- El análisis de comportamiento de la red (NBA).
- El sistema de prevención de intrusiones inalámbricas (WIPS).

Descripción

Contextualización:

En la actividad 1 se identificaron las diversas amenazas y vulnerabilidades de la universidad y por tal el papel como analista de seguridad es realizar las recomendaciones para estos eventos, por tal es necesario planificar, mejorar o implementar las medidas necesarias para proteger tanto la parte física como la parte de la información, recordando que la información que no está segura puede ser factor de riesgo CRITICO para cualquier institución.

Actividad:

Con base en la Actividad 1 por cada amenaza o vulnerabilidad encontrada investigar, sustentar y redactar al menos una recomendación para proteger, mejorar o monitorear dichos eventos y con ello evitar las fuentes de ataque e intrusión (por ejemplo: base de datos, DNS, keylogger e ingeniería social entre otras).

Se analizaron los descubrimientos hechos en la actividad 1, se documentó sobre recomendaciones y se les proporcionaron a la institución educativa en la tabla de recomendaciones. Es necesario revisar el documento y asignar personal responsable de atender dichas recomendaciones y poder cubrir esas observaciones realizadas.

Justificación

En esta actividad continuaremos con lo detectado en la actividad 1. Con el descubrimiento realizado, realizaremos 2 recomendaciones por tipo de las detecciones:

- Amenazas Humanas :

  Ausencia de controles de acceso en el área administrativa y financiera.

  Uso de los equipos para actividades personales, aumentando la exposición a malware.

- Amenazas lógicas:

  Uso de software descargado de internet sin verificar la fuente en el servidor 2.

  Firewall deshabilitado, dejando vulnerable la red.

- Amenazas físicas:

  Entradas múltiples sin controles estrictos ni alarmas de seguridad en áreas importantes y sensibles.

  Extintores clase A y B, no aptos para incendios eléctricos.

- Vulnerabilidades de almacenamiento:

  Equipos sin almacenamiento suficiente.

  Base de datos general en un servidor vulnerable, expuesto a ataques debido a la falta de seguridad perimetral.

- Vulnerabilidades de comunicación:

  Ancho de banda de 20 Gb comercial, insuficiente para las operaciones de una institución.

  Falta de segmentación de la red, lo cual facilita los ataques laterales.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/Seguridad-Inform-tica-1

Desarrollo

Tabla de análisis

A partir de los descubrimientos realizados en la actividad 1, se revisaran 2 amenazas o vulnerabilidades por tipo y se realizaran recomendaciones para protegerlo, mejorarlo o monitorear dichos eventos.

A continuación se presenta la tabla de análisis con sus respectivas recomendaciones para que esos riegos o vulnerabilidades sean solventados por personal de la institución educativa.

Amenazas Humanas	
Ausencia de controles de acceso en el área administrativa y financiera	
Factor Riesgo	El area administrativa financiera no cuenta con una alarma de seguridad para su acceso
Recomendación	● Aplicar segmentación de roles y permisos, donde solamente los usuarios autorizados puedan acceder a las áreas críticas. ● Implementar sistemas de biometría y cámaras de seguridad para restringir la entrada a las áreas administrativas y financieras, Site de los servidores, etc. ● Ofrecer cursos sobre los riesgos asociados con el ingreso de personal no autorizado a áreas críticas.
Fuente de ataque e intrusión	Amenaza interna y externa, se puede tener acceso a información privilegiada, robo e interrupción de servicios.
Uso de los equipos para actividades personales, aumentando la exposición a malware.	
Factor Riesgo	No se tiene denegado el uso del equipo para actividades personales.
Recomendación	● Establecer normativas que prohíban el uso personal de los equipos corporativos. ● Implementar herramientas de respaldos para la prevención de perdida de información. ● Implementar herramientas de monitoreo para supervisar el uso indebido de los equipos. ● Ofrecer cursos sobre los riesgos asociados con el uso indebido de equipos corporativos.
Fuente de ataque e intrusion	Ingeniería social, comprometer los sistemas críticos, robo e interrupción de servicios y tener acceso a información delicada.

En el caso de las amenazas Humanas se dio recomendaciones sobre la falta de controles de accesos al área administrativa y financiera. Cabe mencionar que dichas recomendaciones deberían ser aplicables también al área Site de servidores. Además se realizó recomendaciones sobre el uso de los equipos de trabajo para actividades personales.

Amenazas Lógicas	
Uso de software descargado de internet sin verificar la fuente en el servidor 2	
Factor Riesgo	El servidor 2 aloja un sistema de control que se descargó de internet y se desconoce la fuente del software
Recomendación	● Los servidores productivos no deben tener acceso a internet iliminado, se deben bloquear las descargas desde sitios no verificados mediante politicas de grupo o filtrado web. ● Crear un inventario de software autorizado y que se halla verificado de que sea seguro. ● Utilizar antivirus para verificar los archivos antes de su instalación. ● Ofrecer cursos de concientizacion sobre los riesgos descargar software no autorizado.
Fuente de ataque e intrusión	Ingenieria social, comprometer los sistemas criticos, robo e interrupcion de servicios y tener acceso a información delicada.
Firewall deshabilitado, dejando vulnerable la red	
Factor Riesgo	El firewall no se encuentra habilitado
Recomendación	● Activación del firewall en todos los equipos y configurar reglas para bloquear accesos no autorizados. ● Implementar herramientas de detección y prevención de intrusiones para monitorear y bloquear actividades sospechosas. ● Instalación de un firewall perimetral para proteger la red completa.
Fuente de ataque e intrusión	Ingeniería social, comprometer los sistemas críticos, robo e interrupción de servicios y tener acceso a información delicada.

En el caso de las amenazas Lógicas se dio recomendaciones sobre el uso de software descargado de internet sin tener ninguna verificación del sitio, de su código, etc. Además se tocó el tema del firewall deshabilitado en los equipos de trabajo y servidores, lo cual representa un riesgo crítico y debe ser remediado de manera inmediata.

Amenazas Físicas	
Entradas múltiples sin controles estrictos ni alarmas de seguridad en áreas importantes y sensibles.	
Factor Riesgo	Presenta una entrada principal, dos laterales y una posterior (no se menciona casetas de entrada y control).
Recomendación	● Implementación de control de acceso, con un sistema biométrico o código en todas las entradas. ● Colocación de cámaras de seguridad en los puntos de entrada y áreas críticas. ● Contratar personal de seguridad para controlar los accesos. ● Implementar un sistema de alarma y un centro de monitoreo interconectados. ● Ofrecer cursos de capacitación para el personal de seguridad.
Fuente de ataque e intrusión	Amenaza a la seguridad personal, daños a la infraestructura y equipos, robo e interrupción de servicios, espionaje corporativo, pérdida de datos e información sensible.
Extintores clase A y B, no aptos para incendios eléctricos.	
Factor Riesgo	Se cuenta con 2 extintores clase A y 1 Clase B en el piso principal
Recomendación	● Distribuir extintores en todas los pisos y que estén correctamente señalizados. ● Reemplazar o complementar los extintores actuales con extintores clase C que son especiales para incendios eléctricos ● Asegurarse que cada extintor este etiquetado (donde indique su clase y su uso específico) además de que sean revisados con periodicidad. ● Capacitar al personal en el uso de extintores.
Fuente de ataque e intrusión	Amenaza a la seguridad personal, daños a la infraestructura y equipos, perdida de datos e Información sensible.

.

En el caso de las amenazas Físicas se dio recomendaciones sobre las entradas múltiples, no solo al edificio sino también a las distintas áreas, donde no se tiene un sistema de armas de vigilancia ni de biometría para accesos autorizados. También se dieron recomendaciones sobre la cantidad, ubicación y tipos de extintores que se encuentran en funcionamiento en la institución, los cuales no son los adecuados ni la cantidad necesaria para poder afrontar una situación en caso de ser necesario.

Vulnerabilidades de almacenamiento	
Equipos sin almacenamiento suficiente.	
Factor Riesgo	Los equipos han estado lentos y se estan quedando sin espacio de almacenamiento
Recomendación	● Realizar una revisión de los dispositivos y sus capacidades ● Establecer políticas para la eliminación de archivos obsoletos o duplicados. ● Implementar servicios de almacenamiento en la nube. ● Agregar discos duros adicionales en los equipos si es posible.
Fuente de ataque e intrusion	Amenaza a la seguridad personal, daños a la infraestructura y equipos, robo e interrupción de servicios, espionaje corporativo, pérdida de datos e información sensible.
Base de datos general en un servidor vulnerable, expuesto a ataques debido a la falta de seguridad perimetral.	
Factor Riesgo	El servidor cuenta con la base de datos general de oracle dabatase en un sistema operativo L
Recomendación	● Mantener el sistema operativo y el software de base de datos actualizado de forma regular. ● Configurar un firewall perimetral con ips autorizadas para limitar el acceso al servidor. ● Habilitar cifrados seguros para proteger los datos críticos. ● Segmentación de red para mayor seguridad. ● Usar herramientas de auditoria y monitoreo para detectar actividades sospechosas. ● Asegurarse que los usuarios y las aplicaciones accedan a la base de datos con los privilegios necesarios mínimos.
Fuente de ataque e intrusion	Ingeniería social, comprometer los sistemas críticos, robo e interrupción de servicios y tener acceso a información delicada.

En el tema de las vulnerabilidades de almacenamiento, es importante que atiendan las recomendaciones dadas, tengan un plan de mantenimiento constante de los equipos, se revisen sus capacidades de acuerdo a su función y trabajo.

En el tema del servidor de base de datos, se entregan las recomendaciones para mantener un servicio seguro, actualizado y con una correcta administración.

Vulnerabilidades de comunicación	
Ancho de banda de 20 Gb comercial, insuficiente para las operaciones de una institución.	
Factor Riesgo	Servicio de internet de 20 Gb comercial
Recomendación	● Realizar una evaluación del tráfico y los requisitos de ancho de banda y estimar el consumo necesario ● Contratar un servicio de ancho de banda empresarial para mayor capacidad y calidad de servicio. ● Implementar políticas de priorización de aplicaciones. ● Acordar con el proveedor niveles de servicios para asegurar la disponibilidad.
Fuente de ataque e intrusion	Perdida de datos e información sensible, interrupción de servicios.
Falta de segmentación de la red, lo cual facilita los ataques laterales.	
Factor Riesgo	No hay segmentacion de la red (todas las areas comparten la misma red)
Recomendación	● Crear segmentación y dividir las redes, según su criticidad y operación. ● Aplicar controles estrictos para eliminar la comunicación entre subredes. ● Crear DMZ para servidores expuestos al público separada de la red interna. ● Implementar sistemas de monitoreo y detección de intrusiones. ● Crear plan de actualización de hardware y software periódicos. ● Crear plan de actualización de hardware y software periódicos. ● Realizar auditorías periódicas para la evaluación de la seguridad del ecosistema. ● Ofrecer cursos de capacitación y concientización para el personal.
Fuente de ataque e intrusión	Ingeniería social, comprometer los sistemas críticos, robo e interrupción de servicios y tener acceso a información delicada.

En el caso de las vulnerabilidades de comunicación detectadas, se realizan las recomendaciones sobre el tema del ancho de banda que tiene la institución el cual debe ser revisado a conciencia y debe realizarse la configuración correcta de seguridad para evitar ataques.

Se revisó la vulnerabilidad de falta de segmentación, la cual es muy importante como en las recomendaciones dadas por nuestra parte, ya que no es buena práctica que áreas de operación normal tengan acceso a redes críticas.

Cabe mencionar que en todos los casos es muy importante cursos de concientización del usuario, para que pueden entender los riesgos asociados a cada una de las detecciones que hemos realizado. El punto más débil siempre va a ser el personal, por eso es importante que se realicen dichos cursos y campañas de revisión de la aplicación de políticas de seguridad por parte de los empleados.

Conclusión

Detectar riesgos y vulnerabilidades es algo que se realiza en nuestro día a día en todos los ámbitos de nuestra vida, como en el personal o familiar, detectamos riesgos, como por ejemplo cerradura de la puerta principal no cierra e intervenimos para reparar dicho riesgo y así evitar una intrusión en nuestro hogar lo que puede llevar a un robo. En el mundo de los negocios es muy importante además de realizar análisis de vulnerabilidades y amenazas, es el realizar recomendaciones para proteger los activos, la información y la operatividad de la organización. Este proceso nos permitirá identificar áreas que pueden estar expuestas o tener una seguridad débil que podrían ser explotadas por atacantes o que pueden provocar incidentes y diseñar medidas para prevenir o mitigar esos riesgos.

En mi experiencia personal siempre en el área donde me encuentro laborando, en la cual se atienden servidores con sistema operativo Windows server, es muy importante esta revisión de la seguridad y robustez de la configuración del sistema operativo como de los aplicativos que viven y funcionan en él, junto con las comunicaciones que tiene dicho sistema o su base de datos con otros ambientes o dispositivos, para lo cual siempre hay un escaneo de riesgos realizado por el área encargada de seguridad la cual al detectar riesgos o vulnerabilidades, realiza el informe sobre dichos riesgos y sus recomendaciones de acuerdo a las mejores prácticas de seguridad, las cuales tienen un tiempo para su remediación de acuerdo a su criticidad y la criticidad del recurso afectado.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/Seguridad-Inform-tica-1

Referencias

Prevención y detección de intrusiones. (n.d.). Fortra.com. Retrieved January 12, 2025, from https://www.fortra.com/es/soluciones/ciberseguridad/infraestructura/deteccion-prevencion-intrusiones

¿Qué es un sistema de prevención de intrusiones? (n.d.). Palo Alto Networks. Retrieved January 12, 2025, from https://www.paloaltonetworks.lat/cyberpedia/what-is-an-intrusion-prevention-system-ips

¿Qué es un sistema de prevención de intrusiones (IPS)? (2024, July 16). Ibm.com. https://www.ibm.com/mx-es/topics/intrusion-prevention-system