Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | # 3| Plan de Acción

Seguridad Informática 1

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Pilar Barajas Cervantes

FECHA: 16/09/2024

índice

Introducción

Un plan de acción de ciberseguridad busca proteger los activos digitales de una organización, mitigando el riego de vulnerabilidades que puedan ser aprovechadas por un adversario. Para implementar un plan de ciberseguridad, se pueden tomar las siguientes medidas.

1. **Capacitar a los empleados. Es importante educar a los empleados sobre los riesgos de seguridad y como mitigarlos.**
2. **Utilizar contraseñas seguras. Es importante utilizar contraseñas robustas y renovarlas periódicamente.**
3. **Mantener los sistemas actualizados. Es importante mantener los sistemas y aplicaciones actualizados y aplicar parches.**
4. **Utilizar un firewall. Un firewall confiable y actualizado puede ayudar puede ayudar a identificar amenazas sospechosas.**
5. **Hacer copias de seguridad. Es importante hacer una copia de seguridad y actualizar constantemente.**
6. **Utilizar inteligencia artificial. La inteligencia artificial puede identificar datos ocultos anomalías en accesos y detectar amenazas más rápidamente.**
7. **Implementar un plan de respuesta a incidentes. Es importante contar con un plan de respuesta incidentes bien definidos para mitigar las consecuencias de un ataque.**

Descripción

En este proyecto final activad 3 después de identificar los factores de riesgo en la actividad 1 y realizar las recomendaciones en la actividad 2 ahora es importante aplicar estos conocimientos demostrando como resolver esos eventos encontrando una solución para cada incidencia encontrada. Contar con un firewall confiable y actualizado ayuda a identificar amenazas y conductas sospechosas, contar con una copia de seguridad y actualizarla constantemente es una de las mejores medidas contra la perdida de información. Realizar este plan de acción ayudará a toda empresa para la que se trabaja a evitar cualquier amenaza. Los riegos de seguridad pueden surgir desde adentro como desde afuera de la organización, por ello las estrategias están enfocadas en el manejo de herramientas y la capacitación del personal de toda empresa.

La evaluación de riesgos para idéntica y abordar las vulnerabilidades de seguridad que pueden ser exportadas por los atacantes. Por ejemplo, pueden descubrir que las contraseñas del equipo son débiles y fácil de adivinar. A demás es valioso para mejorar la confianza de los clientes, socios y reguladores ya que la empresa está tomando medidas para proteger sus datos. Idealmente se debe de evaluar los riesgos por lo menos una vez al año, y con mayor frecuencia si se experimentan cambios significativos en la infraestructura o negocio. las organizaciones que están expuestas a un mayor riesgo, así como las que manejan datos sensibles o que operan en industrias reguladas pueden necesitar evaluaciones más frecuentes.

Justificación

Un plan de reforma de respuesta a incidentes permite a los equipos de ciberseguridad limitar a prevenir daños. El objetivo de la respuesta a incidentes es prevenir a los ataques cibernéticos antes que ocurran y minimizar el costo de la interrupción del negocio resultante de cualquier ataque cibernético que ocurra. Idealmente una organización define los procesos ante incidentes en un plan de formal de respuesta a incidentes (IRP) que especifica exactamente como deben identificarse contenerse y resolverse los diferentes tipos de ciberataques. Un plan eficaz de respuesta a incidentes puede ayudar a los equipos de ciberseguridad a detectar y contener las ciber amenaza y restaurar los sistemas afectados más rápido y reducir la pérdida de ingresos y otros costos asociados con estas amenazas.

Un incidente de seguridad, o evento de seguridad es cualquier violación digital física que amenace la confidencialidad, integridad o disponibilidad de los sistemas de información o datos confidenciales de una organización. los incidentes de seguridad pueden variar desde ciberataques intencionales por parte de los hackers o usuarios no autorizados algunos incidentes de seguridad comunes incluyen.

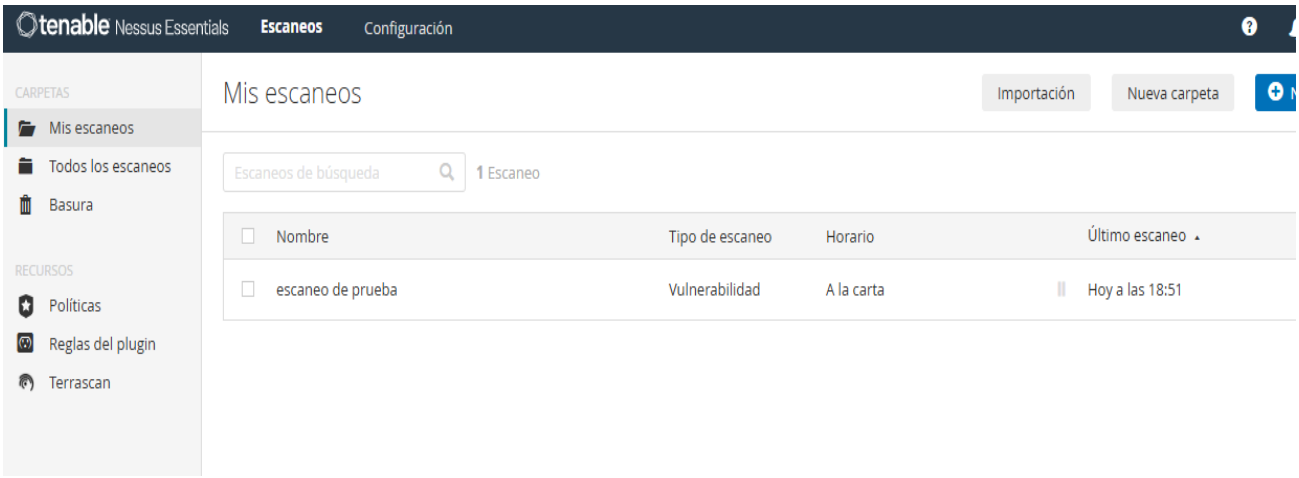
1. **Ransomware**
2. **Phishing e ingeniería social.**
3. **Ataque DDoS**
4. **Ataque a la cadena de suministro.**
5. **Amenazas internas.**

Selección de software

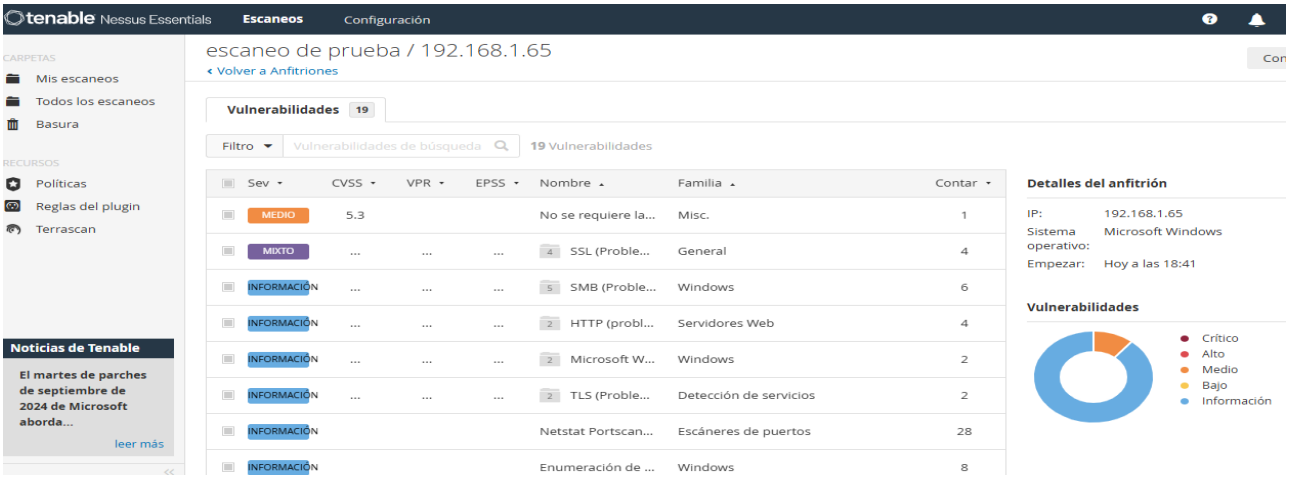
En esta ocasión utilizaremos el software Nessus ya que es una herramienta de escaneo de seguridad remota que analiza vulnerabilidades en sistemas operativos.

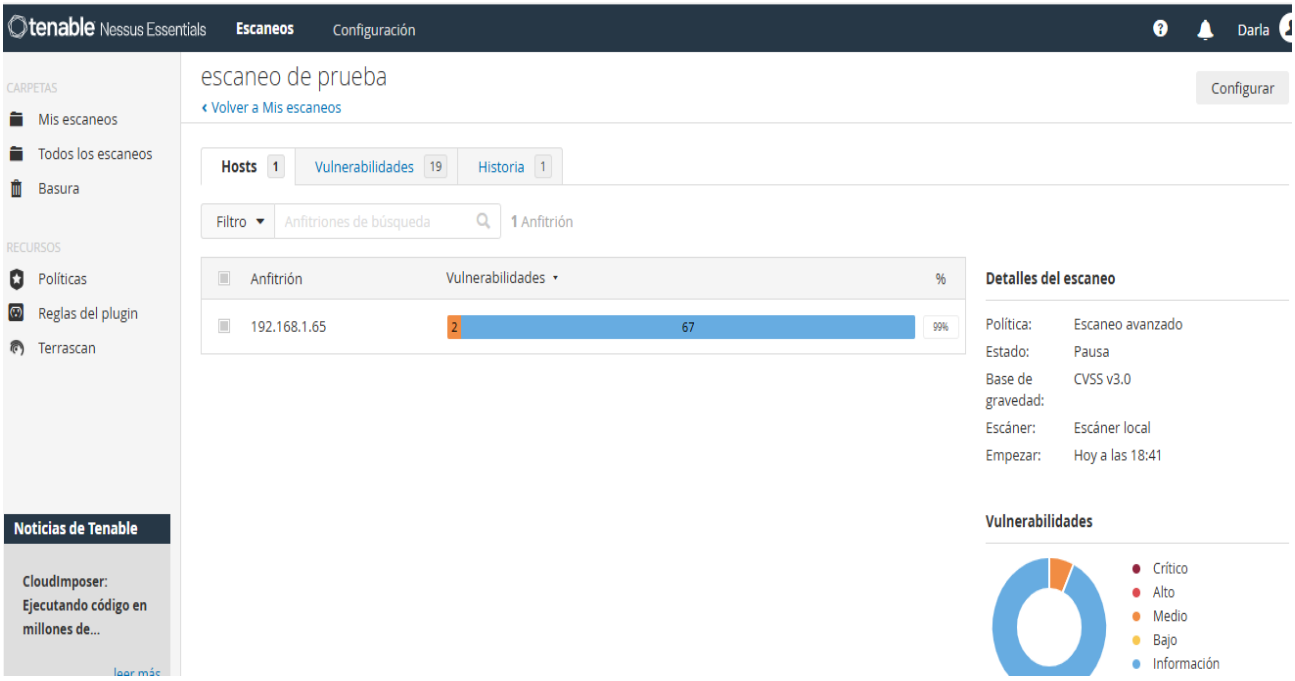
Instalación Nessus

Como primer paso comenzaremos el escaneo de las vulnerabilidades que se encuentran en nuestra IP.



En esta imagen podemos encontrar las vulnerabilidades en contradas en una IP.





Plan de acción

	Semana 1	Semana 2	Semana 3	Semana 4
Incidencia	Equipos lentos	Contraseñas básicas	Desconocimiento del software	Firewall inhabilitado
Solución	Para evitar que los equipos se vuelvan lentos cada cierto tiempo se realiza el mantenimiento es decir limpiar equipos actualizar sistemas y verificar el modo seguro.	Generar contraseñas diferentes en cada equipo de trabajo y realizar el cambio en periodos constantes esto ayudará a evitar las fuentes de ataques e itruisión.	todo el peronal de nuevo ingreso tiene que tener la información necesariá de software utilizado ya que esto evitara a no caer en las amenazas logicas del mundo cibernetico.	realizar la configuración de firewall esto puede ayudar a que se bloquen las nuevas amenazas o los nuevos tipos de tráfico comercial.
Fechas	1 al 30 de septiembre 2024	1 al 31 de cada mes	1 al 5 de cada mes	de 3 a 5 años
Herramienta	https://netable.com	https://netable.com	https://netable.com	https://netable.com

Practicas plan de acción

	Mes			
	Semana 1	Semana 2	Semana 3	Semana 4
Mantenimiento de equipos				
Generar contraseñas seguras				
Capacitación de nuevo personal				
Configuración del firewall				
Limitar acceso a BD				
Configurar conexiones a Wi-Fi seguras				
Instalación de antivirus a todo el equipo de trabajo				
Instalar alarmas de seguridad				
Denegar acceso a todo empleado no autorizado				
Contar con dispositivos para las amenazas físicas				
Actualizar sistema				
limpiar equipo de trabajo				

Conclusión

El plan estratégico de ciberseguridad es un proyecto que propone una serie de medidas que ayudan a reducir los riesgos en entorno a la ciberseguridad de una empresa. Deben contener los aspectos técnicos, legales u organizativos que deben llevar a cabo para reducir los riesgos provocados por las amenazas que afectan a una compañía en un nivel aceptable. Un plan estratégico de ciberseguridad tiene que ayudar a establecerla estrategia que se tiene que implementar incluyendo las medidas técnicas, legales y organizativas adecuadas. La estrategia nos permite focalizar los esfuerzos donde realmente es necesario dentro de la organización, permite aunar esfuerzos entendiendo los objetivos de la medida de seguridad se ha implementado, también nos permite identificar las amenazas y priorizarlas según su riego es la plaza central de la estrategia no se puede establecer una estrategia sin entender el negocio y sus procesos.

En el ámbito de la ciberseguridad la estrategia de la ciberseguridad permite aprovechar y focalizar los recursos disponibles en las áreas de mayor riesgo para que sean más rentables. Conocer la parte estratégica es esencial para desarrollar cualquier plan eso si no hay que dejar de lado el conocimiento más técnico de la ciberseguridad para poder generar un plan completo y realista. El objetivo de todas las organizaciones deberían ser la reducción de sus ciber riesgos lo máximo posible o al menos, hasta un umbral asumible por el negocio, no existe el riesgo cero, con lo que, las compañías adopten todo tipo de medidas o controles de seguridad preventivos, deben de existir planes de detección, respuestas y recuperación para minimizar el impacto en caso de incidente.

Referencia

Blog | Euncet | Centro universitario y escuela de negocios. (2024, 23 julio). Euncet Business School. https://blog.euncet.com/

Inicio | My Site 3. (s. f.). My Site 3. https://seguridadinformatica.com/

Thomson Reuters Mexico. (2022b, febrero 18). Thomson Reuters México - Respuestas confiables. https://www.thomsonreutersmexico.com/