Basque CyberSecurity Centre

Gestión de Vulnerabilidades cheat sheet

1. Definición

Proceso que consiste en identificar, evaluar, tratar e informar los riesgos de seguridad que presentan los sistemas y software de una organización. Conocido como ***"Vulnerability Management"***.

Este proceso, implementado junto a otras medidas de seguridad, consigue que las organizaciones tengan "controladas" aquellas fuentes de posibles ataques, pudiendo centrar su atención en reforzar la seguridad en dichos sitios.

El plan de gestión debe ser revisado y actualizado periódicamente por la alta dirección, lo que ayudará a mejorar la protección de los datos de la organización.

2. Proceso de Gestión

Identificación

Paso crítico. Una buena identificación es clave para el análisis de amenazas y establecimiento de controles de mitigación.

Herramientas / Opciones identificación vulnerabilidades:

Escáneres de red. Identifican todos los sistemas conectados y los analizan en busca de vulnerabilidades.

- **¿Como?** Envió paquetes TCP/UDP ó ejecución PINGs.
- **Tipo:** Internos (pruebas y ataques desde la propia red) y externos (investigador simula ataque desde el exterior).
- **Herramientas.** Nmap, OpenVAS, ...

Instalación de agentes. Monitorización continua del dispositivo. Facilitan la creación de informes y obtención de métricas.

- **¿Cómo?** Instalación de agente en dispositivo.
- **Herramientas.** Kismet, Tenable, ...

Evaluación

Identificadas las debilidades y su información relacionada, comienza el proceso de valoración. Será necesario evaluar cada una de las debilidades encontradas para establecer prioridades y centrar la atención en aquellos riesgos que pongan en peligro la continuidad de la organización.

- Revisar resultados eliminando posibles falsos positivos
- Utilizar un sistema de evaluación, por ejemplo, matriz probabilidad/impacto.
  - Facilita identificación visual riesgos críticos
  - Clasificación amenazas en base a probabilidad de que ocurra e impacto sobre organización
  - Establecimiento umbral de riesgo aceptable

Matriz probabilidad-impacto		IMPACTO				
		Muy bajo (0.1)	Bajo (0.2)	Medio (0.3)	Alto (0.4)	Muy alto (0.5)
PROBABILIDAD	Muy baja (0.1)					D 0.05
	Baja (0.2)	C 0.02			B 0.08	
	Media (0.3)	E 0.03				
	Alta (0.4)	A 0.04				
	Muy alta (0.5)					

Tratamiento de las vulnerabilidades

Seleccionar la estrategia de tratamiento:

- **Evitación o eliminación del riesgo.** Eliminar el activo que produce el riesgo hará que la amenaza desaparezca.
- **Mitigación del riesgo.** Aplicar medidas o controles para reducir el riesgo hasta un nivel aceptable.
- **Transferencia del riesgo.** Transferir el riesgo a una tercera parte u organización.
- **Aceptación del riesgo.** Aceptar que el riesgo existe y no realizar acción. Útil cuando una vulnerabilidad se considera de bajo riesgo y el costo que supondría corregirla es muy superior al efecto que tendría.
- **Remediación del riesgo.** Solventar o parchear la vulnerabilidad en su totalidad siempre que sea posible.

Una vez que el tratamiento se ha completado es aconsejable la verificación ejecutando otro análisis de vulnerabilidad para asegurar que se ha mitigado o remediado.

Notificación

Generar informe de resultados

Los resultados del análisis de vulnerabilidades deben de ser publicados en la organización para:

- Concienciar de los peligros presentes.
- Facilitar la identificación de riesgos futuros.
- Establecer medidas, técnicas y herramientas remediación de riesgos.
- Comprender el porqué de los riesgos.

Generar plan de remediación

Desarrollar y ejecutar un plan de gestión de vulnerabilidades que permita corregir los aspectos identificados y evaluados en función de la prioridad establecida con la matriz de probabilidad/impacto.

3. Herramientas

Software diseñado para analizar de forma automática cualquier sistema o red en busca de posibles vulnerabilidades que puedan afectar a la seguridad de la organización.

NMAP

- Herramienta más usada para identificar hosts dentro de una red local. También permite la identificación de hosts en Internet para comprobar si están conectados a la red.
- Permite realizar escaneo de puertos para identificar servicios operativos sin protección del FW
- Código abierto y multiplataforma. Más habitual uso Linux como pentesting.

OpenVAS

- Permite su ejecución tanto dentro como fuera de la red a analizar, simulando un ataque externo.
- Genera un informe completo con el detalle de vulnerabilidades identificadas y los riesgos para nuestro sistema.
- Permite su configuración para monitorización continua, estableciendo umbrales y alertas.

Tenable (Nessus)

- Basado en agentes.
- Estos recolectan información de vulnerabilidades, configuraciones incorrectas (cumplimiento de la configuración referencias CIS) y datos del sistema y reportan dicha información al Nessus Manager ó al Tenable.io para su análisis.
- Facilita cuadros de mando para la monitorización y plantillas de informe para la notificación de los resultados.