Plan para el análisis de seguridad de un SI basado en Wordpress

Enunciado:

---

1. Elabora un plan para el análisis de seguridad de un sistema de información basado en Wordpress.

Paso 1: Recopilación de información

Se llevarán a cabo las siguientes indicaciones:

- **Identificar Usuarios y Roles:** Identificar a todos los usuarios que interactúan con el sistema y asigna roles y privilegios específicos a cada uno
- **Documentar Políticas de Seguridad:** Revisar y documentar todas las políticas de seguridad existentes en el sistema, como políticas de contraseñas, políticas de acceso y políticas de retención de datos.
- **Evaluar Procesos de Negocio:** Si el sistema está vinculado a procesos de negocio, evaluar cómo el sistema contribuye a esos procesos y cómo los procesos impactan en la seguridad del sistema.
- **Inventario de Datos Sensibles** Identificar y clasificar los datos sensibles o críticos que se almacenan o procesan en el sistema. Esto puede incluir datos personales, financieros o cualquier otro tipo de información confidencial.
- **Identificar Recursos Críticos** Enumerar los recursos críticos para el funcionamiento del sistema, como servidores, bases de datos, aplicaciones específicas y cualquier elemento que, si falla, podría tener un impacto significativo en la operación.
- **Flujos de Datos** Mapear los flujos de datos a través del sistema para comprender cómo se mueve la información entre los componentes y los usuarios.
- **Identificar Dependencias Externas** Identificar cualquier servicio, componente o sistema externo en el que el sistema confía, como servicios de terceros, APIs o servicios en la nube.
- **Historial de Incidentes** Revisar el historial de incidentes y problemas anteriores relacionados con el sistema para obtener información sobre problemas de seguridad previos.
- **Diagrama de Red:** Si el sistema está en una red, crear un diagrama de red que muestre la topología de la red y cómo el sistema se relaciona con otros sistemas y dispositivos.

Paso 2: Identificación de amenazas

La identificación de amenazas implica identificar los eventos o escenarios que pueden poner en peligro la seguridad del sistema.

Las etapas para la deteccion de amenazas serán las siguientes

- **Identificar y enumerar las amenazas cibernéticas específicas** que podrían afectar al sistema. Esto puede incluir:
    1. Ataques de fuerza bruta.
    2. Ataques de inyección SQL en WordPress o al Sistema Gestor de Base de Datos.
    3. Ataques de denegación de servicio (DDoS) contra el servidor servidor web que aloje la web.
    4. Malware y virus que podrían infectar el sistema.
- Considerar amenazas físicas, como incendios, inundaciones, robos o daños en el hardware del servidor
- Incluye amenazas relacionadas con errores humanos, como la configuración incorrecta de permisos de archivo, contraseñas débiles o la posibilidad de que un empleado realice acciones maliciosas.
- Examinar las amenazas internas, que pueden ser tanto intencionales como no intencionales
- Considerar amenazas relacionadas con el cumplimiento de normativas y regulaciones, como multas por incumplimiento de la privacidad de datos.
- Identificar amenazas externas, como la posibilidad de que un atacante externo comprometa la seguridad a través de Internet.
- Evaluar las amenazas naturales, como terremotos, tormentas o inundaciones, que podrían afectar la ubicación física del sistema.
- **Escenarios de Amenaza:** Para cada amenaza identificada, crear escenarios de amenaza específicos que describan cómo podría ocurrir la amenaza y qué impacto tendría en el sistema.
- **Priorización de Amenazas:** Clasificar las amenazas identificadas según su probabilidad de ocurrencia y su impacto en el sistema. Esto ayudará a centrar tus esfuerzos en las amenazas más críticas.

Paso 3: Identificación de vulnerabilidades

3.1. Se utilizarán herramientas de escaneo de seguridad como Wordfence Security para identificar vulnerabilidades conocidas en WordPress y sus componentes (plugins, temas, núcleo).

Wordfence Security (Plugin de WordPress): es un popular plugin de seguridad para WordPress que incluye un escáner de seguridad en tiempo real. Puede escanear tu sitio web en busca de vulnerabilidades conocidas, malware y otros problemas de seguridad. Además, ofrece cortafuegos y otras características de seguridad.

3.2. Verificar si se están utilizando versiones actualizadas de WordPress, plugins y temas.

3.3. Realizar pruebas de penetración para descubrir vulnerabilidades no conocidas.

Para ello se seguirán los siguientes pasos

- **1:** Definir el alcance de las pruebas
- **2:** Obtener el consentimiento y autorización
- **3:** Recopilar información
- **4:** Identificar posibles puntos de entrada
- **5:** Realizar pruebas de seguridad:
  - **5.1.** Escaneo de vulnerabilidades automatizado
  - **5.2.** Pruebas de inyección de SQL
  - **5.3.** Pruebas de cross-site scripting o request forgery (XSS, CSRF)
  - **5.4.** Pruebas de autenticación y autorización
- **6:** Documentar resultados
- **7:** Informar y remediar
- **8:** Realizar pruebas de confirmación
- **9:** Revisión continua

Paso 4: Análisis de controles

El análisis de controles implica evaluar los mecanismos de seguridad existentes en el sistema para determinar si son adecuados para mitigar las amenazas y las vulnerabilidades identificadas previamente. A continuación, se detallan los pasos para llevar a cabo esta etapa:

- **Enumerar Controles Existentes:** Identificar y enumerar todos los controles de seguridad existentes en el sistema. Esto incluye controles técnicos (firewalls, antivirus, sistemas de detección de intrusiones), controles de políticas (políticas de acceso, políticas de contraseñas) y procedimientos operativos.
- **Evaluar la Efectividad:** Evaluar la efectividad de cada control en relación con las amenazas y vulnerabilidades identificadas. ¿Los controles están diseñados adecuadamente? ¿Están configurados correctamente? ¿Están actualizados?
- **Identificar Brechas en los Controles:** Identificar cualquier brecha o deficiencia en los controles actuales que no sean adecuados para mitigar las amenazas o las vulnerabilidades identificadas.
- **Políticas de Seguridad:** Revisar y evaluar las políticas de seguridad existentes para garantizar que sean apropiadas y estén alineadas con las necesidades del sistema y las mejores prácticas de seguridad.
- **Evaluación de Procesos:** Evaluar los procesos de seguridad existentes, como la gestión de parches, la gestión de incidentes y las políticas de gestión de usuarios, para asegurarte de que sean efectivos y estén alineados con los objetivos de seguridad.
- **Verificación de Cumplimiento:** Asegurarse de que todos los controles y políticas estén en cumplimiento con las regulaciones y normativas aplicables, como el RGPD, HIPAA o cualquier otro estándar relevante.
- **Revisión de Configuración:** Verificar que las configuraciones de seguridad, como cortafuegos, listas de control de acceso y configuraciones de seguridad de aplicaciones, estén configuradas correctamente y sean coherentes con las mejores prácticas de seguridad.
- **Evaluación de Acceso y Autorización:** Evaluar los sistemas de acceso y autorización para asegurarte de que solo los usuarios autorizados tengan acceso a recursos y datos específicos.
- **Identificación de Controles Faltantes:** Identificar cualquier control de seguridad que pueda faltar y que sea necesario para mitigar riesgos específicos. Estos controles faltantes pueden incluir la implementación de autenticación de dos factores o la configuración de copias de seguridad regulares.
- **Informe de Análisis de Controles:** Documenta los resultados de tu análisis de controles, resaltando las áreas donde los controles actuales son efectivos y donde pueden necesitar mejoras.
- **Recomendaciones de Mejora:** Basándote en el análisis, haz recomendaciones específicas para mejorar o fortalecer los controles de seguridad existentes.

Paso 5: Determinar la probabilidad de ocurrencia

En esta etapa, se evaluar la probabilidad de que ocurran las amenazas identificadas. La probabilidad se puede estimar de diversas formas, tanto cualitativas como cuantitativas. A continuación, se describen los pasos para determinar la probabilidad de ocurrencia:

- **Análisis Cualitativo:** Esto implica calificar la probabilidad como baja, moderada o alta, basándote en tu conocimiento y experiencia. Por ejemplo, si sabes que tu sistema está bien protegido y monitoreado, es posible que califiques la probabilidad de un ataque DDoS como baja.

- **Análisis Cuantitativo:** Esto implica utilizar datos numéricos para calcular la probabilidad de ocurrencia. Por ejemplo, podrías calcular la probabilidad de un ataque de fuerza bruta en función de la tasa de intentos de inicio de sesión fallidos en el pasado.
- **Revisar Estadísticas:** Si es posible, revisa estadísticas históricas de amenazas y ataques similares en sistemas similares. Esto puede proporcionar una base sólida para estimar la probabilidad.
- **Consultar a Expertos:** Puede ser útil consultar a expertos en seguridad cibernética o a profesionales de tu organización para obtener sus opiniones y evaluaciones sobre la probabilidad de ocurrencia.
- **Utilizar Datos de la Industria:** Algunos sectores y organizaciones publican informes sobre amenazas y vulnerabilidades comunes. Estos informes pueden proporcionar información valiosa para estimar la probabilidad.
- **Asignar Niveles de Probabilidad:** Para cada amenaza identificada, asigna un nivel de probabilidad apropiado. Esto puede expresarse como una probabilidad en porcentaje o en una escala cualitativa.

Paso 6: Análisis de impacto

El análisis de impacto implica evaluar las consecuencias o el impacto que tendría la materialización de una amenaza en el sistema. A continuación, se describen los pasos para llevar a cabo esta etapa:

- **Identificación de Escenarios de Impacto:** Para cada amenaza identificada, crear escenarios de impacto específicos que describan cómo afectaría la amenaza al sistema en términos de funcionalidad, integridad, confidencialidad y disponibilidad.
- **Evaluación del Impacto:** Evaluar el impacto potencial en el sistema en cada uno de estos aspectos. Cómo afectaría la amenaza la capacidad del sistema para funcionar, la integridad de los datos, la confidencialidad de la información y la disponibilidad de los recursos.
- **Clasificación del Impacto:** Clasificar el impacto en una escala, como bajo, moderado o alto, para cada aspecto evaluado. Esto ayudará a entender la gravedad de las consecuencias.
- **Priorización de Escenarios:** Priorizar los escenarios de impacto en función de su gravedad y su probabilidad de ocurrencia. Algunos escenarios pueden tener un impacto menor pero una alta probabilidad, mientras que otros pueden tener un impacto catastrófico pero una baja probabilidad.
- **Documentación del Análisis de Impacto:** Documentar los resultados del análisis de impacto, resaltando los escenarios de mayor preocupación y sus consecuencias.

Paso 7: Determinación de riesgo:

La determinación de riesgo implica calcular el nivel de riesgo asociado a cada amenaza identificada. Este cálculo se basa en la probabilidad de ocurrencia y el impacto que discutimos en los pasos anteriores. Aquí tienes cómo llevar a cabo esta etapa:

- **Calcular el Riesgo:** Calcula el riesgo para cada amenaza multiplicando la probabilidad de ocurrencia (estimada en el paso 5) por el impacto (evaluado en el paso 6). La fórmula básica sería → Riesgo = Probabilidad x Impacto.
- **Clasificar el Riesgo:** Clasifica el nivel de riesgo resultante en una escala, como bajo, moderado o alto, para cada amenaza. Esta clasificación se basa en umbrales predefinidos que tu organización puede establecer.
- **Priorizar el Riesgo:** Prioriza las amenazas según su nivel de riesgo. Esto te ayudará a identificar las amenazas que requieren una atención inmediata y aquellas que pueden abordarse en un segundo plano.
- **Documentación del Riesgo:** Documenta los resultados de la determinación de riesgo en un formato que sea fácil de entender para las partes interesadas. Esto puede incluir tablas, gráficos o informes que resuman los niveles de riesgo para cada amenaza.
- **Comunicación de Riesgos:** Comunica los niveles de riesgo a las partes interesadas y asegúrate de que todos comprendan cuáles son las amenazas más críticas y los riesgos asociados.
- **Revisión Continua:** Recuerda que el riesgo puede cambiar con el tiempo debido a factores como la evolución de las amenazas, las actualizaciones del sistema y las medidas de mitigación implementadas. Por lo tanto, es importante revisar regularmente la determinación de riesgo y actualizarla según sea necesario.

Paso 8: Recomendaciones de control

Las recomendaciones de control son las medidas específicas que se deben tomar para mitigar o gestionar los riesgos identificados en la evaluación de riesgos. Aquí están los pasos para llevar a cabo esta etapa:

- **Priorizar Recomendaciones:** Basándote en la determinación de riesgo realizada previamente, prioriza las recomendaciones de control. Comienza con las amenazas que tienen un mayor riesgo y trabaja hacia abajo en la lista.
- **Detallar Medidas de Control:** Para cada amenaza o vulnerabilidad, proporciona recomendaciones específicas sobre las medidas de control que deben implementarse. Estas medidas pueden incluir acciones técnicas, políticas, procedimientos y cambios en la configuración.
- **Especificar Responsabilidades:** Asigna responsabilidades claras para la implementación de cada medida de control. Debe quedar claro quién es responsable de llevar a cabo cada tarea.

- **Definir Plazos:** Establece plazos realistas para la implementación de cada medida de control. Esto ayudará a garantizar que las acciones se tomen en un período de tiempo adecuado.
- **Establecer Indicadores Clave de Desempeño (KPI):** Define KPIs para medir el éxito de la implementación de cada medida de control. Estos indicadores permitirán evaluar si las medidas son efectivas en la reducción de riesgos.
- **Presupuestar Recursos:** Estima los recursos necesarios, como personal, tecnología o presupuesto, para llevar a cabo las medidas de control recomendadas. Esto ayudará a garantizar que haya recursos disponibles.
- **Documentar Detalles Técnicos:** Si las recomendaciones incluyen cambios técnicos, como actualizaciones de software, configuraciones específicas o parches de seguridad, documenta estos detalles técnicos de manera clara y precisa.
- **Revisión y Validación:** Antes de la implementación, revisa y valida las recomendaciones para asegurarte de que sean apropiadas y factibles.
- **Presentar a las Partes Interesadas:** Comunica las recomendaciones de control a las partes interesadas relevantes, incluyendo a los tomadores de decisiones y a los equipos técnicos encargados de la implementación.
- **Seguimiento y Cumplimiento:** Realiza un seguimiento de la implementación de las medidas de control y asegúrate de que se cumplan los plazos y se alcancen los KPIs establecidos.

Paso 9: Educación y concienciación

9.1. Capacitar a los administradores y usuarios sobre buenas prácticas de seguridad.

9.2. Fomentar la identificación de posibles amenazas y cómo informarlas.

Paso 10: Documentación del resultado

La documentación del resultado es una etapa crítica para garantizar que todos los hallazgos y conclusiones de la evaluación de riesgos estén debidamente registrados y comunicados a las partes interesadas. Aquí están los pasos para llevar a cabo esta etapa:

- **Elaborar un Informe de Evaluación de Riesgos:** Crear un informe detallado que resuma todos los hallazgos y resultados de la evaluación de riesgos. El informe debe ser claro, conciso y fácil de entender para las personas que lo leerán.
- **Incluir Resumen Ejecutivo:** Comienzar con un resumen ejecutivo que proporcione una visión general de los resultados clave y las recomendaciones más importantes. Esto es útil para los tomadores de decisiones que pueden no tener tiempo para revisar el informe completo.
- **Describir la Caracterización del Sistema:** Documentar la caracterización completa del sistema, incluyendo la arquitectura, los componentes, las interfaces y cualquier otro detalle relevante.
- **Enumerar Amenazas e Identificar Vulnerabilidades:** Presentar una lista de las amenazas identificadas y las vulnerabilidades del sistema. Incluír una descripción de cada amenaza y su relación con el sistema.
- **Analizar Controles Existentes:** Detalla los controles de seguridad existentes en el sistema y evaluar su efectividad para mitigar las amenazas y vulnerabilidades identificadas.
- **Probabilidad de Ocurrencia e Impacto:** Presentar los resultados de la estimación de la probabilidad de ocurrencia y el análisis de impacto para cada amenaza. Esto puede incluir gráficos o tablas que muestren la relación entre estos dos factores.
- **Determinación de Riesgo:** Proporcionar una clasificación del nivel de riesgo para cada amenaza, basada en la probabilidad y el impacto. Esto puede incluir una matriz de riesgos que muestre visualmente la prioridad de cada amenaza.
- **Recomendaciones de Control:** Describir las recomendaciones específicas para abordar las amenazas y vulnerabilidades identificadas. Cada recomendación debe ser clara, factible y priorizada según la gravedad.
- **Conclusiones y Recomendaciones Finales:** Resumir las principales conclusiones de la evaluación de riesgos y las acciones que deben tomarse para mejorar la seguridad del sistema.
- **Evidencia y Datos de Soporte:** Proporcionar evidencia de respaldo, como resultados de escaneos de seguridad, registros de eventos o cualquier otro dato relevante que respalde tus hallazgos.
- **Distribución y Presentación:** Distribuír el informe a todas las partes interesadas pertinentes y presentar los resultados en reuniones o presentaciones si es necesario. Asegúrate de que las partes interesadas comprendan los riesgos y las medidas de control recomendadas.
- **Mantenimiento y Actualización:** Mantener un registro de versiones del informe y actualízalo según sea necesario a medida que cambien las circunstancias o se implementen medidas de seguridad adicionales.

Paso 11: Implementación de medidas correctivas

11.1. Implementar las recomendaciones y medidas correctivas identificadas durante el análisis.

11.2. Realizar pruebas posteriores a la implementación para verificar la efectividad de las soluciones aplicadas.

Paso 12: Monitoreo continuo

12.1. Establecer un sistema de monitoreo continuo para detectar y responder a amenazas en tiempo real.

Una buena implementación poría ser un SIEM (Security Information and Event Management)

Configurar una solución SIEM, como Splunk o Elastic SIEM, que recopile, correlacione y analice registros de seguridad y eventos en tiempo real. Esta herramienta puede alertar sobre actividades sospechosas, como intentos de inicio de sesión fallidos, accesos no autorizados o cambios en archivos críticos. Además, puede automatizar respuestas a incidentes, como el bloqueo de direcciones IP maliciosas o la notificación de alertas a un equipo de seguridad.

12.2. Mantenerse actualizado sobre las nuevas vulnerabilidades y amenazas de seguridad que puedan afectar a WordPress y sus componentes.