29 de Mayo, 2017

MODELO ESTÁNDAR DE ANÁLISIS DE VULNERABILIDADES

1. INTERACCIONES PREVIAS AL ANÁLISIS

Acciones que se deben tomar antes de iniciar el análisis de vulnerabilidades

A. Descripción del proyecto

i. ¿Por qué es importante hacer el análisis?
ii. Detalle de las acciones que se van a llevar a cabo y su relevancia para el proyecto
iii. Detalle el alcance del análisis (máquinas y dispositivos a incluirse)
iv. Posibles resultados del análisis
v. Detalles del tipo de reportes que se generaran
vi. Los pasos a seguir después del análisis

B. Recabar los permisos y vistos buenos pertinentes

i. Recabar de la dirección el permiso, por escrito, para ejecutar el análisis
ii. Recabar el visto bueno del Departamento de Sistemas
iii. Establecer fechas que sean convenientes para la empresa
iv. Alertar a quien sea pertinente de las fechas y alcance del análisis

2. RECOLLECIÓN DE INFORMACIÓN

Descripción de la información que será recolectada como preámbulo del análisis.

A. Información respecto a las direcciones IP que están visibles a la Internet

i. Información que provea la empresa misma
ii. Información proveniente de fuentes públicas
iii. Información proveniente de instituciones reguladoras de la Internet
iv. Información proveniente de las redes sociales

B. Información respecto al personal de la empresa

i. Información proveniente de fuentes públicas
ii. Información proveniente de instituciones reguladoras de la Internet
iii. Información proveniente de las máquinas de búsqueda
iv. Información proveniente de los bancos de correo electrónico
v. Información proveniente de sitios web de la empresa

C. Modelaje de Amenazas

i. Enumeración de máquinas y/o dispositivos con IP visible a la Internet
ii. Incremento de privilegios dentro de la red interna de la empresa y/o máquinas y dispositivos

D. Análisis de Vulnerabilidades

i. Enumeración de vulnerabilidades que existan
ii. Clasificación de la severidad de las vulnerabilidades
iii. Sugerencias de remedios o soluciones

E. Reportes y Conclusiones

i. Reportes a Nivel Ejecutivo
    1. *Impacto a la empresa*
    2. *Personalización*
    3. *Efectos en el negocio*
    4. *Efectos a los resultados*
    5. *Efectos a la estrategia del negocio*
    6. *Modelo de madurez*
    7. *Lista de riesgos*
ii. Reportes técnicos
    1. *Identificación de problemas sistémicos y análisis de las raíces de las causas*
    2. *Modelo de madurez*
    3. *Aspectos técnicos*
iii. Descripción
    1. *Tomas de pantallas*
    2. *Asegurar que todas las vulnerabilidades están remediadas*
    3. *Capturas de todas las solicitudes/respuestas*
    4. *Ejemplos de puntos de contacto*
    5. *Asegurar que los códigos de remedio provean una validación benigna de la falla*
    6. *Casos de prueba reproducibles*
iv. Determinar las acciones a seguir y proyectos para remediar las vulnerabilidades