UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 2:

Identificación y Mitigación de Riesgos de Seguridad

Sesión 2:

Diseño de un plan de mitigación

OBJETIVO DE LA SESIÓN:

Diseñar un plan básico de mitigación de riesgos para un entorno organizacional sencillo.

Actividad: Detectando SPAM y SMISHING con IA

En colab escribe un programa que detecte mensajes de SPAM y SMISHING. Utiliza la base de datos: SMS PHISHING DATASET FOR MACHINE LEARNING AND PATTERN RECOGNITION

Objetivo de la actividad:

- Reconocer características clave de mensajes que permiten clasificarlos como HAM (legítimos), SPAM (correo basura), o SMISHING (fraude vía SMS).
- Construir y entrenar un modelo de machine learning (Random Forest, SVM o Red Neuronal) con un dataset real.
- Probar textos de ejemplo y propios en un programa en Colab que extraiga automáticamente indicadores como:
    - Palabras sospechosas frecuentes
    - Presencia de URL
    - Presencia de direcciones de correo electrónico
    - Presencia de números de teléfono o dígitos
- Evaluar el desempeño del modelo con métricas de clasificación y reflexionar sobre qué señales son más útiles en la predicción.

Actividad: Detectando PHISING con IA

En colab escribe un programa que detecte mensajes de SPAM y PHISHING. Utiliza la base de datos: https://www.kaggle.com/datasets/juanagsolano/spam-email-from-enron-dataset

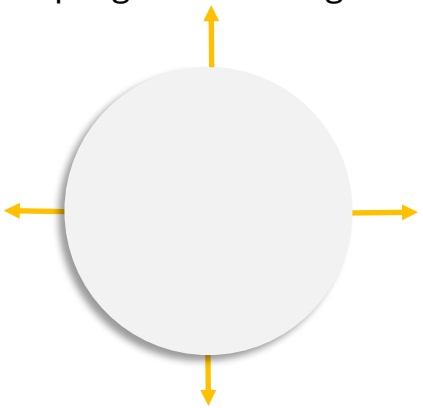
¿Qué es la mitigación de riesgos?

Acciones que reducen la probabilidad de que ocurra un incidente o su impacto si llega a suceder.

Opciones comunes de tratamiento de riesgo

Evitar: Eliminar la actividad que genera el riesgo.

Reducir: Implementar controles para bajar su probabilidad o impacto.



Aceptar: Decidir asumirlo, cuando es menor.

Transferir: Pasarlo a un tercero (ej. seguros).

Pasos para diseñar un plan de mitigación básico

Identificar activos	¿Qué información o sistemas son valiosos? • **Ejemplo:** Base de datos de clientes, servidores, credenciales de acceso.
Identificar amenazas y vulnerabilidades	¿Qué puede afectarlos y cómo? **Ejemplo:** Phishing, ransomware, fallas eléctricas.
Analizar impacto y probabilidad	**Ejemplo:** Ransomware Impacto alto, probabilidad media.
Diseñar controles o acciones de mitigación	**Ejemplo:** Implementar backups automáticos, capacitar a usuarios.
Monitorear y actualizar	Revisar periódicamente si las acciones siguen siendo efectivas.

Ejemplo Guiado

Caso: Pequeña empresa de ventas online
Activo crítico: Base de datos de clientes (datos personales y de tarjetas).
Amenaza: Phishing y ransomware.
Vulnerabilidad: Usuarios sin capacitación y sin backups.
Impacto: Muy alto (pérdida de confianza, legales, operativos).

Plan de mitigación propuesto:

- Implementar políticas de contraseñas seguras.
- Hacer respaldos diarios en la nube.
- Realizar capacitaciones de phishing.
- Activar autenticación multifactor en el servidor de ventas.

Ejercicio 1: Diseño de plan de mitigación

Instrucción: Forma grupos y diseñen un plan de mitigación para el siguiente escenario:
Situación:
Una universidad detecta que sus estudiantes usan contraseñas débiles y comparten sus cuentas para acceder a la plataforma académica, aumentando el riesgo de filtración de calificaciones y datos personales.

1. Identifiquen los activos involucrados.
2. Describan la amenaza y su vulnerabilidad asociada.
3. Analicen el impacto y probabilidad.
4. Propongan al menos tres acciones de mitigación.

Ejercicio 2: Debate grupal

Preguntas:

- ¿Qué tan preparados creen que están sus entornos actuales frente a estas amenazas?
- ¿Qué es lo primero que implementarían como solución de bajo costo?

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. *mishra, sandhya; Soni, Devpriya (2022), "SMS PHISHING DATASET FOR MACHINE LEARNING AND PATTERN RECOGNITION", Mendeley Data, V1, doi: 10.17632/f45bkkt8pr.1*
6. Aguilar, J. (2021). *Spam email from Enron dataset [Data set].* https://www.kaggle.com/datasets/juanagsolano/spam-email-from-enron-dataset