Laboratorio 2

Deivis J. Castro

TALLER – Diferenciar entre Confidencialidad, Integridad y Disponibilidad

Análisis Comparativo:

Actividad:

− ¿Cómo un fallo en la confidencialidad puede comprometer la integridad de los datos?

R: Cuando la confidencialidad se ve comprometida, los datos pueden ser accesibles para actores malintencionados. Si un atacante accede a información sensible sin autorización, puede modificarla, alterando su integridad. Por ejemplo, en un sistema financiero, si una brecha permite a un intruso modificar registros de transacciones, la información deja de ser confiable.

− ¿Cómo la falta de disponibilidad puede afectar la integridad y confianza en los datos?

R: La falta de disponibilidad impide que los usuarios accedan a la información cuando la necesitan. Esto puede provocar pérdida de datos o inconsistencias si los sistemas no están operativos para validar, actualizar o proteger la información. Por ejemplo, en una base de datos de pacientes, si el sistema no está disponible y los registros deben ingresarse manualmente, hay un riesgo de errores y pérdida de información, afectando su integridad y fiabilidad.

Preguntas de Reflexión:

• Pregunta 1: ¿Qué concepto consideras más crítico en una empresa de salud? ¿Y en una empresa de comercio electrónico?

R: En una empresa de salud, la integridad es esencial para garantizar que los datos médicos sean precisos y no alterados, pues decisiones médicas dependen de ellos. Además, la confidencialidad es fundamental para proteger la privacidad de los pacientes.

En una empresa de comercio electrónico, la disponibilidad es crucial, ya que los sistemas deben estar operativos en todo momento para procesar ventas, pagos y logística. La confidencialidad también es clave para proteger datos financieros de los clientes.

• Pregunta 2: ¿Cómo podrías priorizar la implementación de estos conceptos en una organización con recursos limitados?

R:

-Autenticación multifactorial (MFA) para fortalecer la seguridad sin grandes costos.

-Cifrado de datos en bases de datos y correos electrónicos.

-Capacitación en seguridad informática para empleados, evitando brechas por error humano.

-Respaldo y redundancia de datos para garantizar disponibilidad y recuperación ante fallas.

-Uso de herramientas gratuitas o de código abierto para monitoreo y protección de sistemas.

LABORATORIO 2 SEGUNDA PARTE

1.Definir los tipos de malware:

-Virus: Programa malicioso que se adjunta a archivos legítimos y se propaga cuando el archivo infectado es ejecutado. Puede dañar sistemas, eliminar archivos o robar información.

-Gusano: Similar a un virus, pero se propaga automáticamente sin necesidad de intervención del usuario. Puede consumir recursos del sistema y causar fallos en redes.

-Troyano: Se disfraza de software legítimo para engañar a los usuarios y permitir el acceso no autorizado a sistemas. Puede instalar puertas traseras para ataques futuros.

-Ransomware: Bloquea el acceso a archivos o sistemas y exige un pago (rescate) para restaurarlos. Es una de las amenazas más peligrosas en ciberseguridad.

-Spyware: Diseñado para espiar la actividad del usuario sin su conocimiento, recopilando información como contraseñas, datos bancarios y hábitos de navegación.

2. Proporcionar Ejemplos de Cómo Afectan a los Sistemas:

-Virus:

*Se adjunta a archivos legítimos y, al ejecutarse, puede corromper datos, eliminar archivos esenciales del sistema o modificar configuraciones críticas.

*Puede ralentizar el rendimiento del equipo al consumir recursos innecesarios.

*Algunos virus desactivan programas de seguridad, dejando el sistema vulnerable a otros ataques.

-Gusano:

*Se propaga automáticamente por redes sin intervención del usuario, saturando el ancho de banda y causando fallos en la conectividad.

*Puede replicarse en múltiples dispositivos dentro de una red, afectando servidores y estaciones de trabajo.

*Algunos gusanos instalan puertas traseras para permitir accesos no autorizados.

-Troyano:

*Se disfraza de software legítimo y, una vez instalado, permite el acceso remoto a atacantes.

*Puede robar credenciales de usuario, como contraseñas y datos bancarios.

*Algunos troyanos instalan otros tipos de malware, como ransomware o spyware.

-Ransomware:

*Cifra archivos del sistema y exige un pago para desbloquearlos, dejando al usuario sin acceso a su información.

*Puede afectar redes empresariales, paralizando operaciones y causando pérdidas económicas.

*Algunos ransomware eliminan archivos si el rescate no se paga en un tiempo determinado.

-Spyware:

*Se ejecuta en segundo plano, registrando pulsaciones de teclado para capturar contraseñas y datos sensibles.

*Puede monitorear la actividad del usuario, recopilando información sobre hábitos de navegación y comunicaciones.

*Algunos spyware desvían datos a servidores externos sin que el usuario lo note.