Laboratorio #2 – Talento Tech **Juan Sebastian Lopez Marquez**

Título del Laboratorio: Diferenciar entre Confidencialidad, Integridad y Disponibilidad

Definición y Ejemplos

Comprender los principios de Confidencialidad, Integridad y Disponibilidad.

Confidencialidad: Esta nos garantiza que la información sea accesible solo para aquellos autorizados. Un ejemplo de esto sería la información personal de ciertos usuarios. En ciertos casos hay datos sensibles que se desea que no sean visibles para una vista general, como la información de un método de pago.

Integridad: Asegurar que la información no sea alterada de manera no autorizada. Un ejemplo para esto seria el acceder a modificar los datos de un super administrador en la base de datos del servidor desde un usuario sin permisos para esto.

Disponibilidad: Garantizar que la información y los recursos estén disponibles cuando se necesiten. Un caso puede ser la necesidad de acceder a recursos de una pagina web en cualquier momento que sean relevantes para su funcionalidad.

Pregunta 1: ¿Qué concepto consideras mas critico en una empresa de salud? ¿Y en una empresa de comercio electrónico?

Rta 1: Lo que mas considero crítico en una empresa de salud seria la confidencialidad, ya que muchos pacientes/clientes no les gustaría que sus datos puedan ser visibles por un tercero. Y para la de comercio electrónico seria la disponibilidad, ya que si estoy comprando un producto no me agradaría mucho la idea de que no responda la pagina/app o al momento del pago de un producto no pueda continuar con este.

Pregunta 2: ¿Cómo podrías priorizar la implementación a una empresa con recursos ilimitados?

Rta 2: Primero se protege lo que, si se ve comprometido, causaría mayor daño: datos sensibles (confidencialidad), sistemas críticos (disponibilidad) y precisión de la información (integridad). La priorización debe enfocarse en mitigar riesgos donde la pérdida o alteración de datos afecte directamente al negocio.

Defina y Ejemplo

Virus: Los virus informáticos son malwares que contienen código con finalidad maliciosa creados para propagarse entre dispositivos, con el objetivo de dañar el sistema, robar información o tomar el control de los dispositivos. Un ejemplo, es ILOVEYOU que se propago en el año 2000, iba disfrazado como una carta de amor, que al abrirse sobrescribía archivos y se enviaba automáticamente a los contactos del usuario.

Gusano: Es un tipo de malware que se caracteriza por su capacidad de replicarse y propagarse automáticamente a través de redes informáticas, sin la necesidad de intervención humana. En 2003, Blaster aprovechó una vulnerabilidad en Windows para replicarse por si solo a través de redes, provocando reinicios inesperados y ralentizaciones en los equipos.

Troyano: Es un tipo se software malicioso que se disfraza como programa legitimo para engañar los usuarios y obtener acceso a sus sistemas. Zeus, Se ocultaba en el sistema, registrando teclas y enviando datos financieros a ciberdelincuentes.

Ransomware: El ransomware es un tipo de malware que retiene datos y dispositivos como rehenes hasta que se paga un rescate. WannaCry en 2017, cifró archivos en más de 150 países y pedía rescate en Bitcoin para recuperarlos. Afectó hospitales, empresas y gobiernos

Spyware: Es un tipo de malware diseñado para acceder a un dispositivo informático sin el consentimiento del usuario y recopilar información del dispositivo y del usuario para enviarla a terceros. CoolWebSearch se infiltraba en navegadores para redirigir búsquedas web, mostrar anuncios y recopilar hábitos del usuario sin consentimiento.

Resultado de Prueba de Conocimiento Cisco Academy – Introducción a la Ciberseguridad