INSTITUTO KHIPU

Semestre I

Sesión #24

CARRERA PROFESIONAL

DESARROLLO DE SISTEMAS DE INFORMACION

MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE HARDWARE Y SOFTWARE

Tema

INTRODUCCIÓN A LAS APLICACIONES DE SEGURIDAD DEL EQUIPO DE CÓMPUTO

INTRODUCCIÓN A LAS APLICACIONES DE SEGURIDAD DEL EQUIPO DE CÓMPUTO

En la actualidad, un gran porcentaje de los ataques informáticos son dirigidos a sitios web de una compañía o las aplicaciones (intranet, herramientas de cambio de contraseña, aplicativos de negocio, entre otras). Pero ¿Qué consecuencias tiene esto? ¿Las aplicaciones nos garantizan seguridad? ¿Cómo lograr proteger mi información?¿Cuáles son las acciones preventivas que puedo realizar?

Consecuencias de un ataque exitoso

Los ataques exitosos a la seguridad en las aplicaciones de una empresa repercuten tanto en la integridad, confidencialidad y disponibilidad de su información sensible, como en la imagen de esta misma en el mercado, afectando de manera considerable la reputación y las finanzas del negocio. La oportuna identificación y corrección constante de las posibles falencias de seguridad en los aplicativos nos permiten ahorrar trabajo, reducir los costos y aumentar la calidad de las aplicaciones productivas.

Debemos ser capaces de garantizar que la seguridad de la información sea parte integral de las aplicaciones a través del ciclo de vida de estas, estimar las condiciones mínimas de seguridad y operación para que cualquier aplicativo pueda ser puesto en producción.

Garantiza la seguridad de las aplicaciones:

Para lograr garantizar la seguridad de la información en las aplicaciones, debemos considerar todos los requisitos de seguridad, tales como:

Análisis de requisitos y especificaciones de la política de Seguridad de la Información.

Mantener seguros los servicios de aplicaciones a través de internet.

Lograr la protección de las transacciones de servicios en las aplicaciones.

También se debe tener en consideración la seguridad en el desarrollo de las aplicaciones, donde lo fundamental es lograr garantizar la seguridad de la información a través de:

- Políticas de desarrollo seguro.
- Procedimientos de control de cambios.
- Revisiones a las aplicaciones al realizar cambios en los Sistemas Operativos de los usuarios.
- Realizar las pruebas funcionales y de aceptación de sistemas correspondientes.

Junto con lo anterior, también se debe considerar la protección de los datos de prueba que se utilizarán durante el desarrollo de las aplicaciones y no menos importante, considerar la seguridad en las relaciones con los proveedores de software, a través de una política de seguridad para las relaciones con terceros o los requisitos mínimos en los contratos que darán el alcance para la tercerización de las aplicaciones del negocio.

Acciones Preventivas:

Para evitar el riesgo que implican los distintos vectores de amenaza sobre las aplicaciones es que este tema se debe tener presente y considerar en varios aspectos, como:

- **Prevención:** Bloquear la explotación de vulnerabilidades de aplicaciones y protocolos de comunicaciones para evitar su uso malintencionado.

- **Detectivo:** Detectar transacciones de aplicaciones y los intentos para explotarlos con fines maliciosos.
- **Forense:** Registrar los datos sobre la actividad de la aplicación que pueden utilizarse para realizar auditorías e investigación de incidentes.
- **Auditoría:** Analizar los aplicativos con el fin de reunir pruebas y evidencias que sugieren que las aplicaciones son seguras y no sean utilizadas o manipuladas por los atacantes.

Tecnologías de apoyo para la seguridad de la información:

Para apoyar la seguridad de la información del negocio existen distintas aplicaciones en el mercado que permiten analizar de forma constante en el tiempo múltiples sistemas y aplicativos que buscan vulnerabilidades existentes y explotables en la infraestructura de la compañía a través de un sistema de puntaje llamada CVSS, el que nos entrega un valor de acuerdo con la criticidad de la vulnerabilidad y posibles vectores de ataque que pueden ser aprovechados por un agente malicioso.

INSTITUTO

KHIPU