Modelo de amenazas PASTA 2024-11-04 #1

Globe Sistemas

Resumen

Se aplicará el uso del marco del modelo de amenazas del Proceso de Simulación de Ataques y Análisis de Amenazas (PASTA). Se determinará si es seguro lanzar una nueva aplicación de compras.

El modelado de amenazas es una parte importante del desarrollo de software seguro. Los equipos de seguridad suelen realizar modelos de amenazas para identificar vulnerabilidades antes de que lo hagan los actores maliciosos. PASTA es un marco utilizado habitualmente para evaluar el perfil de riesgo de las nuevas aplicaciones.

Escenario

Como parte del equipo de seguridad de la StartUp Globe Sistemas, nos estamos preparando para lanzar una aplicación móvil con IA para ayuda HelpDesk.

Usted está realizando un modelo de amenazas de la aplicación utilizando el marco PASTA. Pasará por cada una de las siete etapas del marco para identificar los requisitos de seguridad de la nueva aplicación de la empresa.

ETAPAS PASTA

Identificar los objetivos del negocio de la APP

El objetivo principal de la Etapa I del framework PASTA es comprender por qué se ha desarrollado la aplicación y qué se espera que haga.

Nota: la Etapa I suele requerir la recopilación de información de muchas personas de una empresa.

En primer lugar, revise la siguiente descripción de por qué la empresa de sistemas decidió desarrollar esta nueva aplicación:

Descripción: Nuestra aplicación debe conectar a la perfección a usuarios y servicio técnico. Debe ser fácil para los usuarios registrarse, iniciar sesión y gestionar sus cuentas. La privacidad de los datos es una gran preocupación para nosotros. Queremos que los usuarios se sientan seguros de que estamos siendo responsables con su información.

Los técnicos deben poder enviar mensajes directamente a los clientes con sus respuestas. También deberían tener la posibilidad de calificar a los técnicos para fomentar un buen servicio. Los tickets de servicio deben ser claros y rápidos de procesar. Los usuarios deben disponer de varias opciones de pago para que el proceso de atención sea fluido. La gestión adecuada de los pagos es realmente importante porque queremos evitar problemas legales.

Evaluar componentes de las aplicaciones

En la Etapa II se define el alcance tecnológico del proyecto. Normalmente, el equipo de desarrollo de la aplicación participa en esta etapa porque es el que tiene más conocimientos sobre la base de código y la lógica de la aplicación. Su responsabilidad como profesional de la seguridad sería evaluar la arquitectura de la aplicación en busca de riesgos de seguridad.

Por ejemplo, la aplicación intercambiará y almacenará muchos datos de los usuarios. Estas son algunas de las tecnologías que utiliza:

Interfaz de programación de aplicaciones (API): Una API es un conjunto de reglas que definen cómo interactúan entre sí los componentes de software. En el desarrollo de aplicaciones, las API de terceros se utilizan habitualmente para añadir funcionalidades sin tener que programarlas desde cero.

Infraestructura de clave pública (PKI): La PKI es un marco de cifrado que asegura el intercambio de información en línea. La aplicación móvil utiliza una combinación de algoritmos de cifrado simétricos y asimétricos: AES y RSA. El cifrado AES se utiliza para cifrar datos sensibles, como la información de las tarjetas de crédito. El cifrado RSA se utiliza para intercambiar claves entre la app y el dispositivo del usuario.

SHA-256: SHA-256 es una función hash de uso común que toma una entrada de cualquier longitud y produce un compendio de 256 bits. La app utilizará SHA-256 para proteger los datos sensibles del usuario, como contraseñas y números de tarjetas de crédito.

Lenguaje de consulta estructurado (SQL): SQL es un lenguaje de programación utilizado para crear, interactuar y solicitar información a una base de datos. Por ejemplo, la aplicación móvil utiliza SQL para almacenar información sobre los servicios que están a la venta, así como sobre los técnicos que las venden. También utiliza SQL para acceder a esos datos durante una compra.

Revisar un diagrama de flujo de datos

Durante la Etapa III de PASTA, el objetivo es analizar cómo maneja la información la aplicación. Aquí se desglosa cada proceso.

Por ejemplo, uno de los procesos de la aplicación podría ser permitir a los clientes buscar en la base de datos los servicios que están a la venta.

Abra el recurso del diagrama de flujo de datos PASTA. Revise el diagrama y considere cómo se relacionan las tecnologías que ha evaluado con la protección de los datos de los usuarios en este proceso.

Nota: Los desarrolladores de software suelen disponer de diagramas de flujo de datos detallados para que los equipos de seguridad puedan utilizarlos y verificar que la información se procesa de forma segura

Utilice mentalidad de atacante para analizar las amenazas potenciales

La Etapa IV consiste en identificar las amenazas potenciales para la aplicación. Esto incluye las amenazas para las tecnologías que enumeró en la Etapa II. También afecta a los procesos de su diagrama de flujo de datos de la Etapa III.

Por ejemplo, el sistema de autenticación de la aplicación podría ser atacado con un virus. La autenticación también podría ser atacada si un actor de amenaza realiza ingeniería social a un empleado.

Consejo profesional: Los registros internos del sistema que utilizará como analista de seguridad son buenas fuentes de información sobre amenazas

Lista de vulnerabilidades que pueden ser explotadas por estas amenazas

La Etapa V de PASTA es el análisis de vulnerabilidad. Aquí, debe tener en cuenta la superficie de ataque de las tecnologías enumeradas en la Etapa II.

Por ejemplo, la aplicación utilizará un sistema de pago. El formulario utilizado para recoger la información de la tarjeta de crédito podría ser vulnerable si no encripta los datos.

En la Etapa V de la hoja de trabajo PASTA, enumere 2 tipos de vulnerabilidades que podrían explotarse.

Consejo profesional: Recursos como la Lista de vulnerabilidades y exposiciones comunes del software

(CVE®) y OWASP son útiles para encontrar vulnerabilidades comunes del software.

Mapa de recursos, amenazas y vulnerabilidades en un árbol de ataque

En la Etapa VI de PASTA, la información recopilada en las dos etapas anteriores se utiliza para construir un Árbol de ataque.

Abra el recurso Árbol de ataque de PASTA. Revise el diagrama y considere cómo los agentes de amenaza pueden explotar potencialmente estos vectores de ataque.

Nota: Las aplicaciones de este tipo suelen tener árboles de ataque grandes y complejos con muchas ramas.

Identificar nuevos controles de seguridad que puedan reducir el riesgo

El Modelo de amenazas PASTA se utiliza habitualmente para reducir la probabilidad de que se produzcan riesgos para la Seguridad. En la Etapa VII, el objetivo final es Implementar defensas y salvaguardas que mitiguen las amenazas.

En la Etapa VII de la hoja de trabajo PASTA, enumere 4 controles de seguridad de los que se haya enterado que pueden reducir las posibilidades de que se produzca un incidente de seguridad, como una violación de los datos.

PASTA WorkSheet

| Etapas PASTA | Globe Sistemas APP |
| --- | --- |
| I. Defina objetivos del negocio y de seguridad | Haga 2-3 notas de requerimientos especiales del negocio que serán analizados.   * La app procesara transacciones? * Realiza la app mucho proceso backend? * Existen regulaciones industriales que deben tenerse en cuenta? * Los usuarios pueden crear perfiles de miembros internamente o conectando cuentas externas. * La aplicación debe procesar transacciones financieras. * La aplicación debe cumplir con PCI-DSS. |
| II. Defina el alcance técnico | Lista de tecnologías usadas por la aplicación:   * Application programming interface (API) * Public key infrastructure (PKI) * SHA-256 * SQL   Las API facilitan el intercambio de datos entre clientes, socios y empleados, por lo que deben priorizarse.  Manejan una gran cantidad de datos confidenciales mientras conectan a varios usuarios y sistemas entre sí.  Sin embargo, se deben considerar detalles como qué API se están utilizando antes de priorizar una tecnología sobre otra.  Por lo tanto, pueden ser más propensas a vulnerabilidades de seguridad porque existe una superficie de ataque más grande. |
| III. Descomponer la aplicación | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| IV. Análisis de amenazas | Enumere 2 tipos de amenazas en PASTA hoja de cálculo que son riesgos para la información siendo manejada por la aplicación.   * Cuales son las amenazas internas? * Cuales son las amenazas externas?Enumere 2 tipos de amenazas en la hoja de cálculo PASTA que representen riesgos para la información que maneja la aplicación. * Inyección * Secuestro de sesión |
| V. Análisis de vulnerabilidades | Enumere 2 vulnerabilidades en PASTA WorkSheet que puedan ser explotadas.   * Podría haber algún problema con el código base? * Podría haber debilidades en la base de datos? * Podría haber fallas en la red? * Falta de declaraciones preparadas * Token de API dañado |
| VI. Modelado de ataque | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| VII. Análisis de riesgo e impacto | Enumere cuatro controles de seguridad que haya aprendido y que pueden reducir el riesgo.   * SHA-256, * Procedimientos de respuesta a incidentes * Política de contraseñas * Principio del mínimo privilegio |