UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ABRIL – AGOSTO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DEL SISTEMA DE SEGURIDAD Y PROTECCIÓN DE DATOS DEL SISTEMA DE SOPORTE OSTICKET, EN LA EMPRESA INGENIERÍA INTEGRASAYOX S.A. UBICADOS EN LA CIUDAD DE BABAHOYO

ESTUDIANTE:

JAZMÍN NOEMI CONTRERAS ANCHUNDIA

TUTOR:

ING. ENRIQUE ISMAEL DELGADO CUADRO

AÑO 2024

Contenido

PLANTEAMIENTO DEL PROBLEMA

Ingeniería Integrasayox S.A., ubicada en la ciudad de Babahoyo, opera en un entorno empresarial competitivo y exigente en términos de calidad de servicio al cliente. Para gestionar eficazmente las solicitudes de los clientes y resolver los problemas técnicos, la empresa utiliza el sistema de gestión de tickets de soporte OSTicket; este sistema es esencial para mantener la operatividad y la satisfacción de los clientes, permitiendo gestionar de forma centralizada todas las consultas y problemas técnicos que surgen a diario, es decir permite el seguimiento de cada paso.

Recientemente, se han identificado varias áreas de mejora relacionadas con la seguridad y la protección de datos en relación con su sistema de soporte técnico, por lo que en primera instancia se ha observado la necesidad de reforzar los mecanismos de autenticación y autorización, lo que resulta crucial para garantizar que solo el personal autorizado tenga acceso al sistema, protegiendo la información sensible tanto de la empresa como sus clientes. Cuando hablamos de la vulnerabilidad en estos sistemas hay que tener en cuenta que podrían ser explotadas, comprometiendo la confidencialidad y la integridad de los datos.

Así mismo, es esencial optimizar los sistemas de copia de seguridad de datos, mejorar estos sistemas es fundamental para evitar cualquier posible pérdida de datos críticos, lo que a su vez garantizará que la empresa pueda responder con eficacia y precisión a las solicitudes de asistencia, se necesita optimizar este sistema ya que es indispensable y así debe asegurar la disponibilidad y precisión de la información en todo momento.

Un aspecto identificado es la mejora de capacitaciones para el personal en temas de la seguridad de la información, las personas son las blandas en la cadena de la seguridad; al no darse una formación adecuada y actualizada puede ser llevado a la práctica insegura como lo es el uso de contraseñas débiles entre otras.

Además, se ha identificado que se debe mejorar a la hora de mantener el software OSTicket y sus componentes auxiliares actualizados con los últimos parches y versiones, proporcionar capacitación continua al personal sobre la practica segura de manejo de datos y respuestas ante incidentes de seguridad, y realizar evaluaciones de vulnerabilidades y pruebas de penetración regularmente para identificar y corregir posibles fallas de seguridad.

La identificación de estas áreas de mejora se ha realizado mediante la observación de las operaciones del sistema, estas observaciones han podido manifestarse y permiten una serie de oportunidades para reforzar las medidas de seguridad actuales.

JUSTIFICACIÓN

La seguridad y la protección de los datos son cruciales para las empresas las cuales manejen información sensible. Examinar el sistema de seguridad y protección de datos del sistema OSTicket en Ingeniería Integrasayox S.A. es fundamental, ya que maneja información sensible tanto a nivel interna como externo; al analizar el sistema de seguridad garantiza que dicha información esté protegida frente a todas las vulnerabilidades como acceso no autorizado, brechas de seguridad y posibles ciberataques. Al implementar medidas de seguridad que sean efectivas se podría desalentar a los atacantes y reducir la probabilidad de incidentes de seguridad.

Además, la confianza de los clientes es un factor principal que se debe de tener en cuenta en cualquier organización, se debe tener la certeza que su información personal está segura y protegida. Al realizar este análisis y optimizar el sistema OSTicket se logrará reforzar la percepción de fiabilidad de la empresa. Un sistema seguro no solo protege la información, sino que también muestra el compromiso con la privacidad y la seguridad de sus clientes; lo que puede ser un factor importante diferenciador en el mercado atrayendo a clientes que valoran la seguridad de sus datos. Además, al mejorar la seguridad del sistema puede generar ventajas competitivas adicionales, una mayor satisfacción y lealtad de los clientes, reducción de costos asociados a brechas de seguridad y la posibilidad de acceder a nuevos mercados en donde se estén necesitando altos estándares de protección de datos.

Estas acciones son esenciales para mantener y mejorar la reputación de la empresa; al incrementar la eficiente y seguridad del sistema ayudara a fortalecer la confianza y satisfacción de los clientes, asegurando la continuidad operativa de la empresa siendo un entorno empresarial cada vez más competitiva y exigente.

Por lo tanto, este estudio de caso se considera suficientemente pertinente, ya que aborda tanto la protección de datos como la mejora de la eficiencia operativa, dos pilares fundamentales para el éxito a largo plazo de la empresa. Visionando estas mejoras, la empresa va a poder anticipar futuras amenazas y adaptarse amenazas y a cambios tecnológicos, asegurando la sostenibilidad y crecimiento en el mercado.

OBJETIVOS

Objetivo general

Analizar el sistema de seguridad y protección de datos de soporte en la empresa Ingeniería Integrasayox S.A. ubicado en la ciudad de Babahoyo.

Objetivos específicos

- Identificar posibles amenazas del sistema OSTicket a través de pruebas de penetración con simulación de ataques.
- Evaluar la efectividad de las medidas de seguridad actuales del sistema OSTicket en Ingeniería Integrasayox S.A. a través de un análisis de vulnerabilidad.
- Proponer las mejoras necesarias, para que el sistema OSTicket funcione en óptimas condiciones, fortaleciendo la seguridad de la información de la compañía.

LÍNEAS DE INVESTIGACIÓN

Línea: Sistemas de Información y Comunicación, Emprendimiento e Innovación

La línea de investigación influye en el trabajo de investigación al centrarse en la evaluación de la seguridad y la gestión de la información dentro del sistema OSTicket; el análisis de vulnerabilidad y la propuesta de mejoras son esenciales para garantizarla confidencialidad, integridad y disponibilidad de los datos elementos fundamentales en esta línea de investigación.

Este análisis busca desarrollar nuevas ideas para mejorar la seguridad de la información, al enfocarnos en emprendimiento aquí fomenta la búsqueda de soluciones innovadoras y sostenibles para abordar los desafíos de seguridad; en la innovación nos orientamos adoptar tecnologías avanzadas y la implementación de mejora continua, para así asegurar que el sistema se logre mantener robusto y competitivo ante nuevas amenazas.

Sublínea: Redes y tecnología inteligente de Software y Hardware

La sublinea de investigación tiene como principal objetivo evaluar y reforzar la infraestructura tecnológica empleada para la gestión de soporte técnico. Se enfoca en la detección de vulnerabilidades en el sistema OSTicket y en la proposición de mejoras especificas en la configuración de hardware y software para garantizar la seguridad y confidencialidad de los datos; también se explora la implementación de tecnologías avanzadas que no solo mejoren la eficiencia operativa, sino que a su vez ayuden a que la empresa este en una posición destacada por la adopción de soluciones innovadoras en la gestión de redes y seguridad.

MARCO CONCEPTUAL

OSTicket

OSTicket facilita a las organizaciones a realizar seguimiento de sus solicitudes de atención al cliente y así asegurarse de que toda actividad se haga en el tiempo establecido; al ser una solución flexible y escalable este se adapta a las necesidades desde pequeñas a grandes compañías, todas las interacciones de soporte se redirigen a un solo lugar lo que facilita que los de soporte técnicos ayuden a los clientes, a la resolución de problemas y al seguimiento de incidencias (Ali & Hussain, 2022).

Características

- OSTicket es de código abierto permitiendo a las empresas acogerlo y personalizarlo a sus necesidades sin costos de licencia.
- La interfaz de usuario no es compleja, esto ayuda a facilitar su adopción y hacer buen uso de parte del personal de soporte.
- Existe comunidades activas de desarrolladores y usuarios que contribuyen al desarrollo y soporte del software.
- Cuenta con medidas de seguridad las cuales son actualizaciones regulares, control de acceso detallado, cifrado SSL/TLS y control de entrada.
- Tiene la función de asignar ticket automáticamente, respuestas y recordatorios lo que ahorrara tiempo y recursos.
- Se puede personalizar e integrar con algunos sistemas y herramientas diferentes que utilizan las empresas.
- Esta desarrollado en lenguaje de programación PHP y utiliza MySQL para el manejo de bases de datos y tecnologías ampliamente utilizadas en las empresas. (Jimenez, 2020)

- El sistema cuenta con una arquitectura MVC(Modelo-Vista-Controlador), en el caso de modelo este maneja una base de datos en donde se almacenan los ticket, usuarios y departamento; en vista aquí muestra la interfaz de usuario, esta incluye los formularios de tickets, la lista entre otros; en controlador este gestiona la creación, actualización y cierre de ticket. Este diseño permite que la arquitectura del software este organizado y eficiente para así facilitar el desarrollo, mantenimiento y escalabilidad.

Beneficios

- Optimizando los procesos de soporte, las compañías pueden reducir los costos operativos asociados con la gestión de solicitudes de soporte; permitiendo a las empresas a reinvertir en otra área, mejorando la competitividad y su rentabilidad.
- Puede manejar grandes cantidades de tickets, esto es una gran ventaja para las empresas grandes solicitudes.
- En el sistema OSTicket se encuentran medidas de seguridad que ayudan a garantizar la protección de datos y su integridad.
- Ayudar proporcionando a las empresas informes detallados para que con este recurso se pueda analizar el rendimiento e identificar falencias, esto es una ventaja para que la compañía pueda tomar decisiones basadas en datos y ver áreas que necesiten mejoras que puede ayudar al proceso de soporte.
- En Ecuador, se ha adoptado por empresas en áreas de tecnología, educación, servicios públicos y privados; para mejorar la eficiencia de sus departamentos de soporte y atención al cliente.
- Hay una gran eficiencia al fortalecer las solicitudes las cuales se envían, para que así el equipo de soporte pueda trabajar de manera más eficiente y organizada.

También debemos de considerar que las empresas implementen buenas prácticas de seguridades las cuales son:

- Capacitaciones a los trabajadores sobre las mejores prácticas de seguridad y cómo se pueda mejorar el manejo de información confidencial.
- Realice copias de seguridad frecuentemente de la base de datos y los archivos del sistema.
- Se debe configurar correctamente los permisos para los archivos y carpetas del servidor.
- Mantener actualizado el software y todas sus dependencias.

Estas acciones garantizan que el sistema sea lo más seguro y que los datos estén protegidos de posibles amenazas (Mehmud, 2020).

La utilización del sistema OSTicket, puede hacer:

Poder abrir los incidentes de forma rápida y sencilla

Hacer consultas del estado de las mismas en cualquier momento

Ayuda a la automatización y así simplifica dicha comunicación entre usuario y soporte

Se obtiene informes detallados sobre los soportes prestado y funcionamiento.

Seguridad y la protección de datos

La seguridad de los datos tiene tres principios básicos, los cuales son la confidencialidad, la integridad y la disponibilidad; estos son importantes para cualquier organización que maneje datos confidenciales; sin estos factores la información puede caer en las manos equivocadas, cambiar o dejar de estar disponible cuando sea necesario.

Para los desarrolladores de OSTicket la seguridad es algo que deben se debe tener muy en cuenta, ya que son ellos quienes han implementado varias medidas para proteger los datos y mantener la integridad del sistema; en estas medidas están las actualizaciones periódicas, utilizan el cifrado SSL/TLS para proteger la comunicación de una validación de entrada para evitar posibles ataques. (Valencia, 2021)

Confidencialidad de los datos

La confidencialidad se centra en proteger la información del acceso no autorizado y garantizar que el personal autorizado tenga el único acceso a la información confidencial, manteniéndola segura. OSTicket, logra esto implementando mecanismos solidos de autenticación de usuarios, tales como contraseñas seguras y autenticación de dos factores (2FA). Además, se utiliza un Control de Acceso Basado en Roles (RBAC), lo cual está permitiendo asignar que los usuarios reciban permisos de acceso de acuerdo a su rol, esto les ayuda a controlar y está limitando el acceso a algunas áreas del sistema a donde el usuario no está autorizados.

Integridad de los datos

La integridad trata de que se debe de proteger la exactitud y garantizar que no se modifique ni se destruyan sin permiso. OSTicket tiene un registro de actividad en el cual están detallados todas las operaciones que se realizan en el sistema, en este están incluida la creación, modificación y eliminación de algún tickets; al tener este registro ayuda a monitorear los cambios y así poder detectar alguna actividad sospechosa, también utiliza la validación de datos para poder garantizar que la información ingresados tenga los formatos y limites definidos, lo cual reduce el riesgo de errores y corrupciones de datos.

Disponibilidad de los datos

La disponibilidad garantiza que toda la información sea accesible y esté disponible para los usuarios autorizados cuando la necesiten; OSTicket implementa copia de seguridad periódicas lo cual asegure que los datos siempre puedan estar disponibles así sea en caso de fallos o desastres del sistema. Además, el sistema se monitorea continuamente y se realiza mantenimiento preventivo para minimizar el tiempo de inactividad y garantizar que funcione cuando los usuarios lo necesiten (Yagual, 2022).

Cómo OSTicket implementa estos principios en su plataforma

Proporciona la autenticación basada en contraseñas y soporta la autenticación de 2F para agregar una capa adicional de seguridad; el control de acceso basado en roles (RBAC) permite definir permisos específicos para diferentes usuarios, asegurando que solo el personal autorizado pueda acceder a información sensible.

También utiliza **cifrado de datos** para proteger la información contra accesos no que no estén autorizados durante la transmisión y almacenamiento; esto incluye el uso de protocolos seguros como SSL/TLS para comunicaciones y cifrado de bases de datos para el almacenamiento.

También realiza **copias de seguridad,** proporciona un mecanismo el cual va a ayudar a realizar una recuperación de la información ante posibles desastres, para poder garantizar que dicha información se restaure de manera rápida si llega a haber alguna pérdida de datos o fallos del sistema. Así mismo se mantiene actualizando y parches de seguridad para así reducir vulnerabilidades conocidas; los desarrolladores de OSTicket siguen ayudando a identificar y solucionar problemas de seguridad.

Así mismo el sistema mantiene un registro detallado de toda actividad, esto incluye accesos, modificaciones y eliminaciones de datos; estos registros son especiales para detectar actividades sospechosas, para realizar investigaciones forenses en caso de que haya incidentes de seguridad.

Estos principios y características aseguran que esta plataforma no solo proteja la confidencialidad de datos, también garantiza una respuesta rápida y efectiva ante alguna incidencia; así este sistema se posiciona como una solución confiable y segura para la gestión de tickets para soporte. (Ordóñez, 2021)

Amenazas y vulnerabilidades

Tipos de amenazas

- **Accesos no autorizados:**

  Esto sucede cuando sin autorización una persona ingresa al sistema y a los datos privados; puede resultar perjudicial porque así tendrían a su disposición la información confidencial, podría manipular los servicios de soporte, y así perjudicara a la empresa comprometiendo la confianza y seguridad del sistema (Williams, 2023).

- **Ataque de Phishing:**

  Es una combinación de ingeniería social e exploit técnicos, esto tiene como objetivo intentar convencer a una víctima a caer en una trampa donde va a dar libre acceso a su información personal, tales como contraseñas o detalles de tarjetas de crédito, así suplantando identidades confiables como bancos, almacenes u otros; OSTicket lo que puede ser un punto débil es enviar correos electrónicos falsos a los usuarios, engañándolos a que revelen sus credenciales de acceso; desde este punto de vista esto podría comprometer el

sistema y acceder a datos personales, lo que pone en riesgo la integridad del servicio (Smith & Thompson, 2021).

- **Malware:**

  Es un software malicioso lo cual puede ser un virus, gusanos u troyanos, se pueden infiltrar en algún sistema para así causar algún daño o robar información valiosa; si un dispositivo con acceso al sistema OSTicket ingresa y está infectado con este software malicioso, es perjudicial ya que podría alterar datos o incluso dañar el sistema, y esto afectaría la seguridad del servicio (Brown & Green, 2022).

Vulnerabilidades posibles del sistema

1. **Cross-Site scripting (XSS):**

Es un tipo de ataque el cual busca las fallas de seguridad en sitos web lo cual va a permitir a los atacantes poner scrips con malicia, al ejecutarse ese sripts está dando la información a sus atacantes; investigaciones recientes han identificado ciertas vulnerabilidades XSS en OSTicket los cuales pueden utilizarse para robar cookies durante el inicio de sesión, redirigir a sitios web maliciosos o realizar otras acciones no autorizadas lo que puede ser perjudicial para la seguridad del sistema (Alsaffar, y otros, 2022).

2. **Autenticación con fallos**

Cuando hablamos autentificación de fallos es un problema que sucede cuando un usuario al querer ingresado al sistema tiene problemas de autenticación; en el sistema OSTicket se han presentado fallos en la autenticación esto ocurre cuando un atacante este intentando ingresar de manera ilegal para así tener el acceso al sistema; en algunos estudio (Chinchilla Salazar, 2023) se han revelado la vulnerabilidad de las contraseñas no seguras, las

cuales pueden ser evadidas por atacantes con habilidades tecnológicas, poniendo así en riesgo la seguridad del sistema.

3. **Vulnerabilidades en plugins y extensiones**

Las extensiones estos son programas o complementos los cuales se añaden a los navegadores, como por ejemplo para bloquear publicidades, las traducciones de páginas, gestionan contraseñas, las cuales pueden mejorar el rendimiento; a diferencia de los plugin que hay mucha similitud, pero están relaciona con contenidos multimedia como el audio. En el sistema OSTicket se pueden introducir agujeros de seguridad adicionales si no se administran adecuadamente; las investigaciones han demostrado que muchos plugins no cumplen las mejores prácticas de seguridad, y eso puede abrir la puerta a ataques que comprometan el sistema central de OSTicket (Briceño, 2021).

4. **SQL injection**

Las vulnerabilidades de inyección SQL permiten a los atacantes ejecutar comandos SQL arbitrarios contra la base de datos de OSTicket; hay ciertas versiones de OSTicket son vulnerables a inyecciones de SQL debido a la entrada del usuario que compromete la integridad de la base de datos.

5. **Divulgar información confidencial**

Se debe de proteger la información y la confidencialidad de datos ya que estos garantizan lo necesario para confiar que la información que se proporciona va a estar segura que dicha información no se vaya a divulgar; al no tener una encriptación adecuada en algunos componentes de OSTicket puede provocar la divulgación de datos sensibles, como la información de clientes y detalles de tickets; investigaciones han encontrado que algunas

versiones de OSTicket no cifran adecuadamente los datos en tráfico de información, lo que los atacantes pueden aprovechar para acceder a información confidencial (Lee & Patel, 2023).

Estrategias de protección y mitigación

Medidas de seguridad

Son acciones dirigidas exclusivamente a resguardar la información que se almacena en cualquier sistema, es necesario que se tomen en cuenta una serie de estrategias y medidas de seguridad para así garantizar la protección de datos contenidos; en el sistema OSTicket estas medidas se centran en la autenticación de usuarios, el control de acceso, el cifrado de datos, las copias de seguridad periódicas y las actualizaciones continuas.

1. **Parches de seguridad o actualizaciones de software**

Los parches de seguridad son actualizaciones específicas las cuales revisan y ven si hay vulnerabilidades; el sistema OSTicket instala parches de seguridad después del su lanzamiento para así proteger el sistema de posibles amenazas (Vieites, 2022). Se debe de mantener el software actualizado para poder proteger el sistema de posibles vulnerabilidades y así se mejore la seguridad completa; OSTicket se actualiza cada cierto tiempo para incluir ultimas mejoras de seguridad y eliminar vulnerabilidad descubierta; los administradores reciben notificaciones sobre las actualizaciones disponibles y los parches de seguridad necesarios para proteger el sistema.

2. **Autenticación de usuario y control de acceso**

Es un proceso de verificar la identidad de un usuario antes de permitir el acceso un sistema; OSTicket utiliza varios métodos que garantiza que los usuarios autorizados sean los únicos los cuales tengan el acceso a él; estos métodos también incluyen creación de contraseñas seguras que deben cumplir con ciertos criterios de complejidad, lo que las hace difíciles adivinar. Además, se

ha incluido la autenticación de dos factores (2FA), esto añade una capa adicional de seguridad al obligar a los usuarios que introduzcan dos métodos de verificación, como una contraseña y un código enviado en mensaje de texto al celular; el control de acceso garantiza que los usuarios tengan acceso solo a los recursos y la información necesaria para completar sus tareas, OSTicket tiene un control de acceso basado en roles (RBAC) para administrar estos derechos de acceso, este permisos solo es para los administradores ellos pueden definir roles específicos, como agentes de soporte, administrador del sistema o clientes, y asignar permisos según las necesidades de cada rol. A los roles se les asignas permisos necesarios de acuerdo a su departamento como realizar los usuarios, como ver, crear, editar o eliminar tickets.

3. **Encriptación de datos y copias de seguridad continuas**

La encriptación de datos protege los datos confidenciales tanto en tránsito como en reposo, garantizado que solo los usuarios autorizados puedan acceder a ellos; OSTicket utiliza protocolos seguros como SSL/TLS para cifrar los datos transmitidos entre los clientes y los servidores y protege los datos durante la transmisión; la información que se encuentra en las bases de datos de OSTicket se encuentra cifrada para poder protegerla contra el acceso no autorizado. (Guevara Aulestia, 2023). Las copias de seguridad continua garantizan que todos los datos sean recuperables en caso de pérdida, OSTicket implementa una sólida estrategia de respaldo para proteger los datos; estas se realizan a intervalos regulares, como diaria o semanal, para minimizar la perdida de datos, las reservas se almacenan en lugares seguras y se cifran para protegerlas contra el acceso no autorizados y así poder garantizar su integridad.

Nmap (Network Mapper)

Es una herramienta invaluable en el campo de la seguridad de redes informáticas; se utiliza principalmente para escaneo de puertos y servicios, lo que permite a los administradores de sistemas y profesionales de seguridad identificar los dispositivos activos en una red y los servicios que utilizan; esta herramienta ayuda a saber los dispositivos que están conectados a la red, que puertos tienen abiertos, que sistema operativo están usando y como está configurada la red, es necesaria para identificar alguna vulnerabilidad que los atacantes puedan aprovechar, ya que puede realizar análisis rápidos y detallados. También proporciona una imagen clara y precisa del estado de la red, lo que permite a los profesionales de la seguridad tomar medidas proactivas para la proteger el sistema. (Palacios, 2020)

OpenVAS (Open Vulnerability Assessment System)

Este es una solución la cual nos brinda una solución completa de vulnerabilidades, ofrece variedad de herramientas y servicios que están destinado para idéntica, clasificar y gestionar las debilidades que se encuentren en sistemas y redes informática; el diseño que tiene facilita la detección de puntos vulnerables en la infraestructura de TI, esto proporciona a los administradores de sistema la información que sea necesaria para poder mitigar esos riesgos y así asegurar la integridad de sus entornos operativos.

OpenVAS tiene una arquitectura el cual incluye un servidor y varios módulos escaneo se complementan para así llevar a cabo evaluaciones, un modulo común es el OpenVAS Scanner realiza los escaneos de vulnerabilidades, otro es OpenVAS Manager este gestiona las configuraciones y dichos resultados de escaneos; además esta solución se apoya en una BD de vulnerabilidades que se conoce como Network Vulnerability Tests (NVTs) este se actualiza frecuentemente lo cual puede incluir amenazas nuevas y descubrir vulnerabilidades.

Nikto

Esta herramienta de escaneo de servidores web que esta desarrollado en Perl lo cual se especializa en identificar vulnerabilidades y configuraciones incorrecta, tiene como objetivo principal dar una evaluación de la seguridad del servidor web; esta herramienta permitirá la evaluación del sistema OSTicket lo cual ayudará a identificar y mitigar los riesgos.

MARCO METODOLÓGICO

Método cualitativo

El método cualitativo es una forma de investigación que se enfoca en entender fenómenos complejos a través de la recolección y análisis de datos no numéricos como es la entrevista, observación y documentación. El método cuantitativo es diferente este se centra en medir y analizar variables numéricas, el enfoque cualitativo busca captar las experiencias humanas y sus respectivos contextos; es flexible, permitiendo adaptación según los descubrimientos emergentes, y proporciona una comprensión profunda de los temas tratados.

Esta investigación adopta un enfoque cualitativo, orientado a la obtención de una comprensión profunda y detallada de las buenas prácticas, percepciones y desafíos relacionados con la seguridad y protección de datos del sistema de soporte OSTicket en la empresa Ingeniería Integrasayox S.A., ubicada en la ciudad de Babahoyo; el método cualitativo es adecuado para explorar fenómenos complejos y proporcionar información detallada a través de recolección de datos no numéricos.

Entrevista

Para la recolección de datos, se utilizarán entrevistas este instrumento nos va a permitir explorar en profundidad los conocimientos y experiencia de los entrevistados, proporcionando flexibilidad para profundizar en temas emergentes durante la conversación.

Se entrevistará a cuatro profesionales con experiencia en tecnología en áreas de seguridad y protección de datos, con la finalidad de conocer y poder tomar en cuenta su experiencia en la seguridad para que se tomen las debidas precauciones con el caso y además comparar esos

resultados para analizarlos y discutirlos; los participantes no forman parte de la compañía Ingeniería Integrasayox S.A., lo que va asegurar una perspectiva objetiva y externa.

Observación

La técnica de observación es un método de recolección de datos cualitativos que se basa en ver y registrar de cerca como ocurren las coas en su entorno natural. Em lugar de depender lo que las personas dicen de acuerdo a sus experiencias, esta técnica permite obtener una visión directa de lo que sucede.

Se empleará la técnica de observación para así tener una visión completa del funcionamiento del sistema OSTicket en la empresa. Para llevar a cabo la observación, lo primordial es coordinar con la empresa Ingeniería Integrasayox S.A. para obtener acceso a los lugares donde se utiliza el sistema OSTicket.

RESULTADOS

Como resultado de este análisis hemos concluido con las pruebas que se recitaban realizar para poder observar las vulnerabilidades que tiene y así que la empresa realice mejoras del mismo, el cual nos ha llevado a lo siguiente:

Un ataque de penetración con metasploit framework, en el cual se está creando un payload malicioso para la hacer el ataque a la computadora local en donde se encuentra el sistema, al sistema OSTicket tener seguridad propia el proceso es tardío ya que esta denegando la entrada a dicho ataque.

Figura 1

Penetración de simulación de ataque

Nota. Fuente: Autora

En esta imagen muestra el resultado del ataque, donde vemos que los asteriscos son los más tardío en responder el ataque mostrando que la seguridad del sistema tiene un grado de seguridad media.

Figura 2

Resultados del ataque

```
[*] 192.168.1.111:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.111:445 - The target is vulnerable.
[*] 192.168.1.111:445 - Connecting to target for exploitation.
[+] 192.168.1.111:445 - Connection established for exploitation.
[+] 192.168.1.111:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.111:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.1.111:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50  Windows
[*] 192.168.1.111:445 - 0x00000010  72 65 6d 69 75 6d 20 37 36 30 30                 remium
[+] 192.168.1.111:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.111:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.111:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.111:445 - Starting non-paged pool grooming
[+] 192.168.1.111:445 - Sending SMBv2 buffers
[+] 192.168.1.111:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer
[*] 192.168.1.111:445 - Sending final SMBv2 buffers.
[*] 192.168.1.111:445 - Sending last fragment of exploit packet!
[*] 192.168.1.111:445 - Receiving response from exploit packet
[+] 192.168.1.111:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
```

Nota. Fuente: Autora

Utilizamos una herramienta la cual es SQLmap la cual proviene de SQL Injection con (Metasploitable), en esta herramienta que nos sirve para atacar y visualizar las vulnerabilidades.

Figura 3

SQLmap ataque y visualizar vulnerabilidades

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.110/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#"
```

```
--cookie "security=low; PHPSESSID=0efec68919f875a47be364c74fa5093b"
```

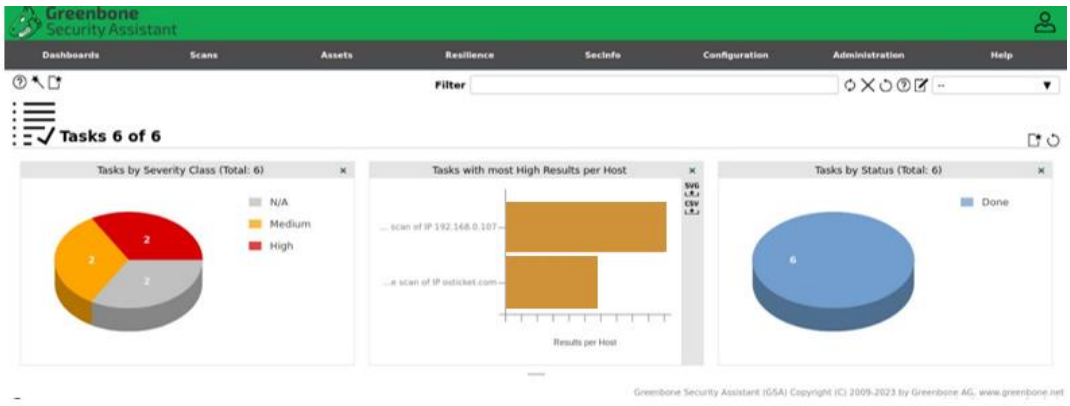
```
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 7735 FROM (SELECT(SLEEP(5)))FRRz) AND

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7170717871,0x666149
it=Submit
---
[00:04:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 5.0.12
[00:04:42] [INFO] fetched data logged to text files under '/home/kali
```

Nota. Fuente: Autora

Utilizamos OPENVAS para realizar un analisis de vulneravilidades de ciertas IP, para que así se veian en las vulnerabilidades mas claras.

Figura 4

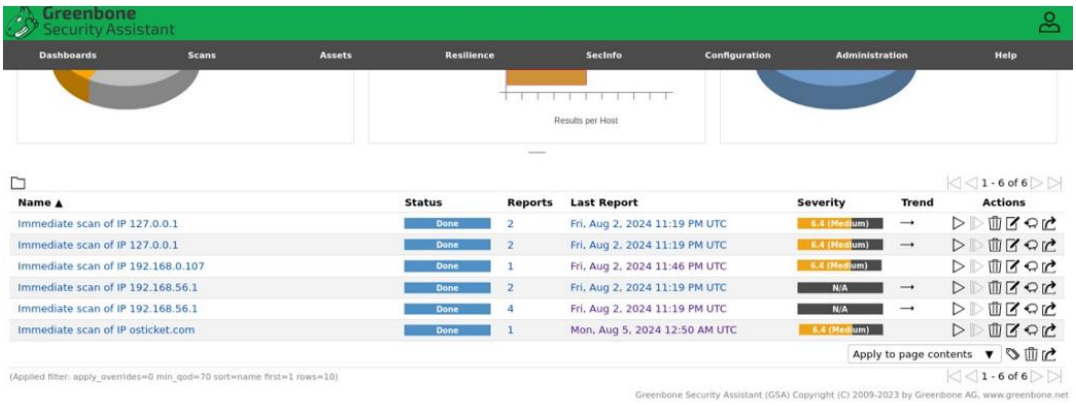
Análisis en OPENVAS



Nota. Fuente: Autora

Figura 5

Muestra los registro e informes del análisis en OPENVAS



Nota. Fuente: Autora

Después que se realizó la penetración del ataque, ahora se realizará el escaneo de red, con la herramienta Nmap, para escanear los puertos posibles que tiene puedan tener abierto y así poder identificar las vulnerabilidades por donde posiblemente puede ser atacada.

Figura 6

Escaneo principal de la red

Nota. Fuente: La autora

Con el nmap -O con la ip del servidor más específicas, para saber cuál es el sistema operativo que está trabajando, pero en este caso no nos está permitiendo saber esa información ya que todos los puertos escaneados están en estado ignorando.

Figura 7

Para verificar las vulnerabilidades del SO

```
Nmap scan report for localhost (127.0.0.1)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 02:27 -05
Nmap scan report for localhost (127.0.0.1)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 02:27 -05
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000081s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

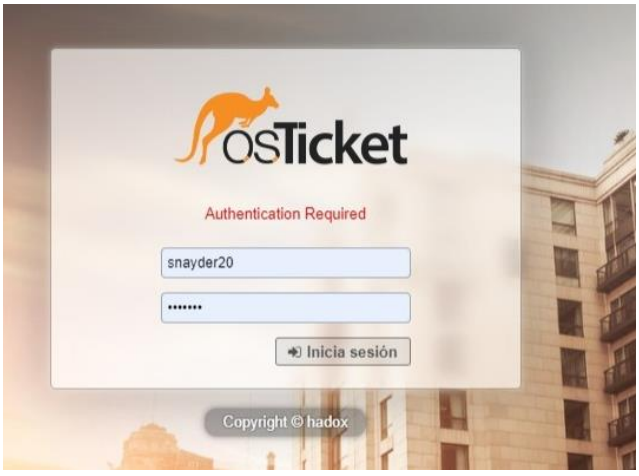
Nota. Fuente: La autora

Las vulnerabilidades del sistema propio

Se mostrará la página principal del sistema de soporte de ticket OSTicket, pero en este caso este inicio de sesión tiene unas pequeñas vulnerabilidades que tiene el sistema ya que en el momento que abandonamos el sistema por un cierto tiempo largo este se vuelve inactivo, pero este es una medida de defensa la cual utiliza para el uso indebido.

Figura 8

Inicio de sección de sistema OSTicket, donde pide autenticación

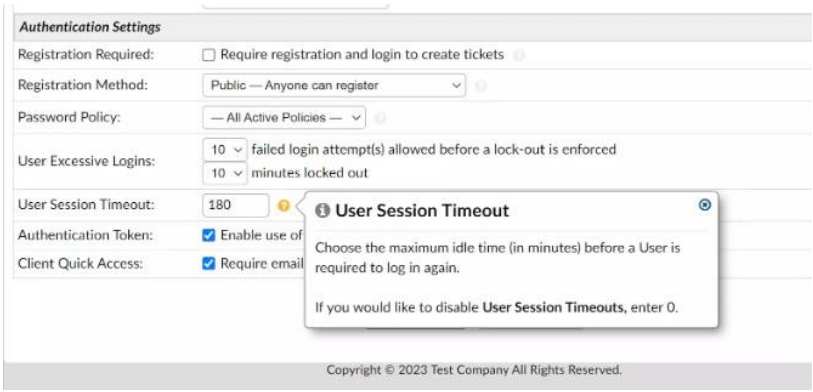


Nota. Fuente: La autora

Aquí se muestra la pantalla donde podemos aumentar el tiempo de inactividad del sistema para que así no exista inconveniente y poder trabajar con normalidad, en este caso este es un método de defensa para que así no ingresen personal no autorizado.

Figura 9

Se ve el aumento de la inactividad



Nota. Fuente: La autora

De acuerdo a la entrevista realizada a los profesionales podemos recalcar sobre la seguridad del sistema, ellos subrayan lo importante que es una infraestructura adecuada en donde se pueda alojar el sistema; ya que al ver un sistema alojado en una PC puede ser vulnerable debido a su infraestructura débil, al contar con un servidor con una solida seguridad ofrece una mejor protección de los datos; una ventaja que tiene este sistema es que es de código abierto lo cual permite que este se personalice para una mejor seguridad, los riesgos que están principalmente son los malware, troyanos, ataques de phishing y el acceso no autorizados lo cual depende de las medidas de seguridad tomadas.

El sistema debe de asegurar confidencialidad, integridad y disponibilidad en el sistema OSTicket, los profesionales recomiendan buenas prácticas, las cuales son la creación de políticas de seguridad claras y específicas, replicación de BD y el uso de contenedores Docker lo cual puede mejorar la disponibilidad así mismo un plan de backups para que se puedan restaurar de manera rápida los datos en caso de algún fallo; el cifrado SSL/TLS y la base de datos, la segmentación de res y el la autentificación fortalecida son medidas que se deben de tener en cuenta.

Al preguntar sobre los incidentes más comunes los profesionales nos mencionan que son los malware, ransomware, troyanos, ataques de phishing, inyección SQL y XSS, ellos recomiendan estrategias efectivas los cuales incluyen implementar programas de capacitación y concientización para la seguridad del usuario, el uso debido de firewalls para que así se pueda proteger la infraestructura perimetral y se pueda realizar revisiones periódicas y detectar dichas vulnerabilidades.

DISCUSIÓN DE RESULTADOS

Al utilizar los métodos y técnicas planteadas en el marco metodológico, se pudo evidenciar los resultados que reflejaron tanto las vulnerabilidades del sistema OSTicket como recomendaciones de los profesionales teniendo en cuenta que los entrevistados tienen experiencia y están al día con la tecnología y con la seguridad que deben de tener los sistemas hoy en día, para salvaguardar la información sensible.

Realizando las pruebas necesarias se evidenció que con la herramienta metasploit el sistema tiene una seguridad de grado media, ya que se observo que algunos componentes estaban lentos en responder a ataque, así se logró identificar posibles áreas de mejora; al utilizar una herramienta de SQLmap este detecto áreas específicas en donde el sistema se podría encontrar en riesgo, ahí destaca la necesidad de la implementación de las medidas de seguridad adicionales para así estar protegido en contra estos ataques; el OPENVAS nos permitió las identificaciones sobre las vulnerabilidades mas claras, esto proporciono un panorama detallado de las debilidades las cuales deben de ser abordadas para así poder reforzar la seguridad del sistema.

En el análisis del escaneo con la herramienta Nmap, nos proporcionó información valiosa para así tener en cuenta cuales son las áreas de mejora que se deben de hacer, en primera instancia como resultado del primer escaneo se pudo evidenciar que existen ciertos puertos abiertos que podrían ser tratados para evitar un ataque malicioso; otro escaneo mostro que el host local está activo y que no existen demoras en la solicitud de red, este es una ventaja en términos de operatividad. Una de las mayores ventajas que se pudo evidenciar es que al momento de querer saber con un escaneo el sistema operativo del servidor nos denegó acceso, no se pudo obtener esa información esto nos indica que el servidor podría estar configurado para así minimizar la exposición de dicha información sensible que maneja el sistema, lo cual es un punto positivo.

Las respuestas que nos proporcionaron se agrupan en diferentes aspectos claves, los cuales son la evaluación general de seguridad del sistema, los riesgos que existen, las vulnerabilidades más importantes y como punto final las recomendaciones que ellos nos dan desde su experiencia en el área para así asegurar la confidencialidad, integridad y disponibilidad de los datos.

Al hablar de la evaluación de seguridad general del sistema, los profesionales enfatizaron en la pregunta dos lo importante que es tener una buena infraestructura del servidor y su seguridad ambiental, en una infraestructura débil ni puede estar alojado un sistema que tenga acceso a datos personales ya que no protegería adecuadamente los datos, también destacan un comentario importante al decir que OSTicket es un sistema de código abierto puede tener un riesgo y una ventaja en el caso de que este no sea manejado profesionalmente; los profesionales identifican posibles riesgos los cuales son intrusos de malware, troyanos y accesos no autorizado a causa de contraseñas débiles y credenciales comprometidas, otro punto es la falta de cifrado también es un riesgo muy importante y al identificar cualquier puerto abierto y al no tomarse las medidas precauciones puede ser una vía para que lleguen los atacantes.

Incluyen recomendaciones donde hablan sobre la implementación de políticas de seguridad especificas algunos de ellos son, el uso de la base de datos de replicación para mayor disponibilidad, el uso de autenticación de dos factores (2FA), un control de acceso basado en roles (RBAC) también un cifrado SSL/TLS para su protección en los datos transmitidos.

CONCLUSIONES

Al combinar las pruebas de penetración, observación y análisis de vulnerabilidad tenemos como conclusión una visión más detallada de la seguridad del sistema OSTicket, hay que hacer énfasis ya que el análisis nos muestra una configuración de seguridad media, hay áreas en donde se requieren mejoras como una seguridad más robusta, los profesionales al proporcionar recomendaciones que junto con un monitoreo continuo y los ajustes de pruebas de vulnerabilidades, nos permitirá que este sistema se fortalezca la seguridad y protección de datos.

El sistema OSTicket en base al análisis que se realizó este está relacionada estrechamente con la seguridad y solidez de una infraestructura que lo alberga, un entorno de seguridad media y vulnerable está exponiendo a múltiples riesgos de seguridad como los ataques los cuales vimos que se pueden ejecutar en contra del sistema y así exista la perdida de datos y acceso no autorizado, los cuales van a afectar la confidencialidad, integridad y disponibilidad de los datos; algo que representa amenazas para el ámbito de la seguridad del sistema OSTicket son los ataques de malware y troyanos lo que hemos hecho la prueba de penetración, hemos visto que estos ataques son perjudiciales porque se filtran en el sistema para cambiar o eliminar datos importantes para así comprometer la integridad del sistema.

El cifrado es indispensable en las comunicaciones y el almacenamiento de datos estos exponen información confidencial a la intercepción y al acceso no autorizado, para así no poner en riesgos la confidencialidad de la empresa y no haya graves consecuencias si los datos caen en manos equivocadas; también la capacitación al personal para mejores practicas los resultados de las pruebas de penetración y análisis de vulnerabilidad nos han indicado que necesitamos fortalecer ciertas áreas en específico; estas mejoras van proteger eficazmente los datos para que así este opere de manera más eficiente.

RECOMENDACIONES

Para mejorar y fortalecer una infraestructura técnica, se debe de implementar servidores virtuales que sean beneficiosos y den buena acogida en la empresa, se necesitan medidas de seguridad, como firewalls avanzados para así proteger el acceso al sistema desde un punto exterior; también se deben de utilizar sistemas de detección y prevención de intrusos para así poder identificar y responder a posibles amenazas. Es importante garantizar que todas las conexiones de red estén muy protegidas con protocolos, para así evitar el acceso que podrían dañar los datos.

La implementación de algunas herramientas de seguridad solida es esencial para ayudar a reducir riesgos, incluye el uso de programas antivirus y antimalware los cuales detecten y eliminen amenazas antes que los ataques maliciosos afecten el sistema; los firewalls deben configurarse ya que ayude a bloquear el tráfico sospechoso y prevenir ataques, al mantener los sistemas actualizados con las últimas versiones de parches de seguridad ayudara a que ataquen.

Es necesario mejorar las políticas de autentificación que tenga la empresa para proteger el sistema; requiere contraseñas que sean complejas no fáciles de descifrar, la autentificación de dos factores agrega una capa adicional las cuales requieren un método de verificación, como el código que suele ser enviado al teléfono, otro factor clave es educar a los empleados sobre la importancia de cambiar las contraseñas cada cierto tiempo; mejorar el cifrado SSL/TLS es fundamental ya que ayuda a proteger los datos que están en curso, este cifrado garantiza que la información que se mueva entre servidores y usuarios está protegida, además el cifrado de la base de datos garantiza que los datos en reposo estén bien protegidos en cualquier caso que exista una violación de seguridad.

REFERENCIA

Ali, M., & Hussain, S. (2022). Análisis de los sistemas de ticketing de código abierto: Un estudio de caso sobre OSTicket. *Journal of Information Technology & Software Engineering*, 85-98.

Alsaffar, M., Aljaloud, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Almurayziq, T. S., Alshammari, G., & Alshammari, A. (2022). Detección de ataques web de secuencias de comandos en sitios cruzados (XSS). *Electronics*.

Briceño, E. V. (2021). *SEGURIDAD DE LA INFORMACIÓN.* Editorial Área de Innovación y Desarrollo,S.L.

Brown, M., & Green, H. (2022). Amenazas de malware en los sistemas de tickets de soporte: Prevención y respuesta. *Information Security Review*, 43-58.

Chinchilla Salazar, M. G. (2023). *Estrategia de fortalecimiento de la gestión de los clientes del sector ornamental que atiende el Laboratorio Fitopatología de la Universidad de Costa Rica mediante un enfoque de CRM.* Costa Rica: SISTEMA DE ESTUDIOS DE POSGRADO .

Guevara Aulestia, D. O. (2023). *Sistema de respaldo de datos utilizando cloud computing para el mejoramiento de la seguridad de la plataforma virtual moodle en la Unidad Educativa del Milenio Intercultural Bilingüe "Chibuleo".* Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Tecnologías de la Información.

Jimenez, L. P. (2020). *Manual tecnico UIFCS.* UIFCS-ALFRESCO.

Lee, H., & Patel, S. (2023). Vulnerabilidades en la exposición de datos en los sistemas OSTicket. *Information Privacy*, 33-48.

Mehmud, T. (2020). osTicket 1.14.2 - SSRF - PHP webapps Exploit. *Open Security*.

Ordóñez, E. A. (2021). *Fundamentos de seguridad informática.* Editorial Grupo Compás.

Palacios, A. P. (2020). *Seguridad informática .* Ediciones Paraninfo, SA.

Smith, J., & Thompson, L. (2021). Ataques de phishing: Repercusiones y contramedidas en los sistemas de venta de tickets. *Cybersecurity* , 56-69.

Valencia, M. E.-P. (2021). La seguridad informática en la adopción del cloud computing en la información del sector industrial . *Revista Ciencia & Tecnología*, 57-71.

Vieites, A. G. (2022). *Audoria de seguridad informatica.* StarBook .

Williams, A. (2023). Acceso no autorizado: Riesgos y mitigación en los sistemas de atención al cliente. *Revista de seguridad informática*, 22-35.

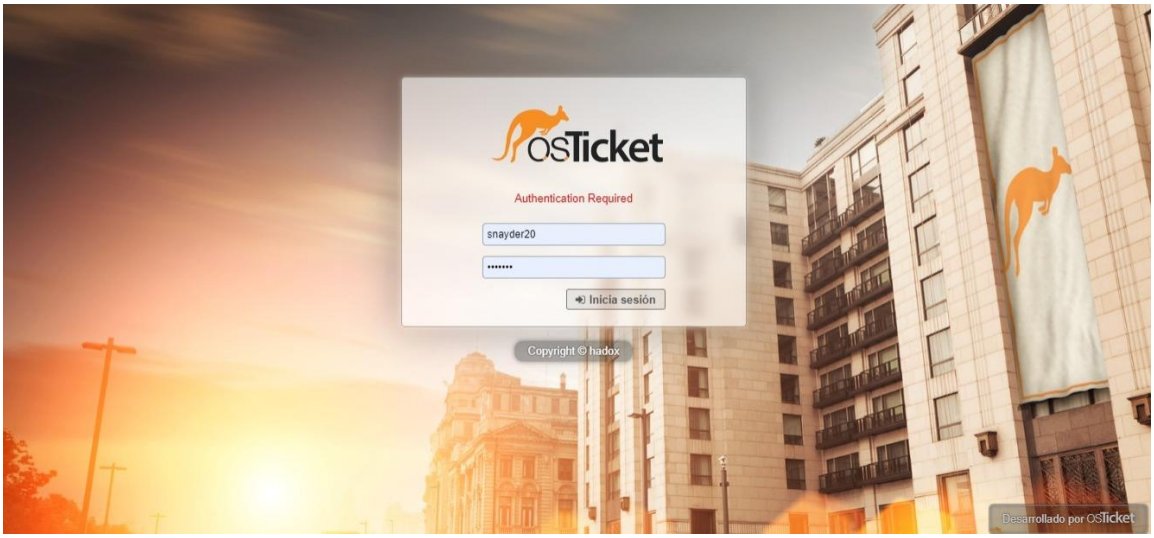
Yagual, I. A. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*, 39-47.

ANEXOS

Sistema OSTicket el cual utiliza la empresa para dar soporte de ticket.

Figura 10

Pantalla de OSTicket



Nota. Fuente: La autora

ENTREVISTA

PREGUNTAS que se realizaron a los profesionales, para su respectiva entrevista son las siguientes:

1) Basado en su experiencia y conocimiento, ¿Cómo evaluaría la seguridad de un sistema de soporte de tickets como OSTicket en términos de protección de datos sensibles, y cuáles son los principales riesgos y vulnerabilidades que debería considerar una empresa que utiliza este tipo de sistema?

2) ¿Qué recomendaciones daría para las buenas prácticas y poder asegurar la confidencialidad, integridad y disponibilidad de un sistema de soporte como OSTicket, y qué medidas específicas de privacidad deberían implementarse?
3) En base a su experiencia, ¿Cuáles son los tipos de incidentes de seguridad más comunes que afectan a los sistemas de soporte de tickets, y qué estrategias de respuestas y mitigación cree que son efectiva para gestionar y prevenir estos incidentes?
4) Desde su perspectiva profesional, ¿Qué políticas y procedimiento de seguridad son esenciales para gestionar y proteger adecuadamente los datos en un sistema de soporte de tickets como OSTicket?

RESPUESTAS

Después de realizar las entrevistas a los profesionales, estos son las RESPUESTAS que nos han proporcionado:

1) Basada en su experiencia y conocimiento, ¿Cómo evaluaría la seguridad general de un sistema de soporte de tickets como OSTicket en términos de protección de datos sensibles, y cuáles son los principales riesgos y vulnerabilidad que debería considerar una empresa que utiliza este tipo de sistema?

   Profesional 1: cuando la seguridad en general tiene algunos aspectos uno de ellos es donde se va alojar el sistema de soporte, si este sistema va a estar funcionando en una PC cualquiera pues seguramente fracasara por tener una infraestructura débil no lograra proteger sus datos de forma adecuada.

   También es necesario evaluar la seguridad perimetral del servidor donde se encuentra alojado, es fundamental que se proteja la base de datos y sitio web de este. Al ser una

plataforma de open source también puede mejorarse la seguridad de forma personalizada, pudiendo también ser esto un riesgo y vulnerabilidad si no se lo trata con profesionalismo.

Profesional 2: la seguridad de los sistemas se puede evaluar a través de herramientas sean de software libre o comercial que permita establecer los riesgos y vulnerabilidades sean del sistema o la base de datos.

Los principales riesgos son la intervención de malware, troyanos que puedan modificar los datos existentes en la base de datos.

Profesional 3: considerando que el sistema OSTicket no tiene como finalidad la seguridad sería conveniente ver los puntos sobresaliente tales como mantener bases de conocimientos, integraciones y la automatización ya que con sus reglas de flujo de trabajo tenemos respuestas rápidas las cuales garanticen el enfoque del sistema y visto de ese punto no sería en tal caso conveniente pero si lo fusionamos con las base de la seguridad ofensiva aplicando de manera acertada el desarrollo de exploits tendremos un apoyo muy importante ya que este se encargaría de la creación de herramientas diseñadas para explorar vulnerabilidades.

Profesional 4: de manera minuciosa se debe de evaluar la seguridad del sistema ya que este maneja datos confidenciales, como son los datos de clientes, la autenticación y la autorización debe de ser clara para así solo los usuarios autorizados puedan acceder a información confidencial. Los principales riesgos y vulnerabilidades son el acceso no autorizado causado por contraseña débiles o credenciales comprometidas, la falta de cifrado adecuado también puede provocar el ataque a los datos que se transmiten.

2) ¿Qué recomendaciones daría para las buenas prácticas y que asegure la confidencialidad, integridad y disponibilidad en el sistema de soporte como OSTicket, y qué medidas específicas de privacidad deberían implementarse?

Profesional 1: para asegurar la confidencialidad puedo recomendar como mejor practica en primer lugar crear una política apegada a este tipo de sistemas que permita amparar a los usuarios que colocan su información en el sistema.

También se puede recomendar mantener base de datos replicadas que permitan una alta disponibilidad utilizando contenedores Docker. Así mismo tener un plan de backups que permita una restauración de contingencia acelerada para que todo funcione sin interrupciones.

Profesional 2: las mejores prácticas que debe tener la organización están dados de acuerdo a las actualizaciones que se puedan realizar en el sistema, teniendo como prioridad el uso de cortafuego (firewalls) para la detección de intrusos al sistema.

Profesional 3: es importante la implementación de cifrado SSL/TS para así proteger los datos en procesos, también cifrar la base de datos para así garantizar que dichos datos confidenciales estén protegidos, hay que establecer derechos de acceso basado en roles para que se limite el acceso a los datos confidenciales que sería solo personal autorizado, tener respaldo y recuperación ante alguna calamidad que pueda suceder como puede ser una falla del sistema

Profesional 4: es necesario para garantizar la confidencialidad, integridad y disponibilidad se recomienda segmentar red para aislar el sistema de otros y así se podría reducir la superficie de ataque, otro punto también es el fortalecimiento de la autenticación. Las medidas que se deben en tomar en cuenta es limitar el acceso de datos, cifrar datos o implementar controles de privacidad

3) En su experiencia, ¿Cuáles son los tipos de incidentes de seguridad más comunes que afectan a los sistemas de soporte de tickets, y que estrategias de respuestas y mitigación considera más efectiva para gestionar y prevenir estos incidentes?

Profesional 1: en relación con los incidentes comunes pues puedo indicar que es muy poca la información que podría existir en relación a esto ya que nadie vulnera sistemas de tickets, nadie quiere vulnerar ni andar hackeando sistemas que no tengan que ver con transacciones o que tengan que ver con dinero de por medio.

Sin embargo, es necesario proteger los datos de los clientes por lo que es necesario una adecuada infraestructura tecnológica virtual que garantice su almacenamiento eficiente y su seguridad perimetral con firewalls. Así como también revisar aspectos de inyección de códigos.

Profesional 2: los tipos de incidentes más comunes son los Malware, Ransower, Troyanos, los cuales tratan de tomar el control de la base de datos.

Profesional 3: los incidentes más comunes que afectan esto sistemas de soporte de ticket es el phishing donde los atacantes obtienen acceso no autorizado mediante fraude y credenciales robadas, otra es los ataques de inyección SQL y XSS son muy comunes estos aprovechan las vulnerabilidades de las aplicaciones para ejecutar código malicioso.

Para ayudar a mitigar eso incidentes es importante la implementación de programas de capacitación y concientización sobre seguridad para que estén al día sobre las amenazas y las mejores prácticas de seguridad.

Profesional 4: hay incidentes que afectan los sistemas de soporte de ticket de manera terrible, algunos de ellos son la violación de datos, malware, ataque web, ataque de phishing e ingeniería social,

4) Desde su perspectiva profesional, ¿Qué políticas y procedimiento de seguridad son esenciales para gestionar y proteger adecuadamente los datos en un sistema de soporte de tickets OSTicket?

Profesional 1: es necesario tener en todas las organizaciones unas políticas de seguridad, se dice que primero es la política y luego la tecnología por lo que es recomendable tener normativas internas que aseguren y garanticen el buen funcionamiento de hardware y software.

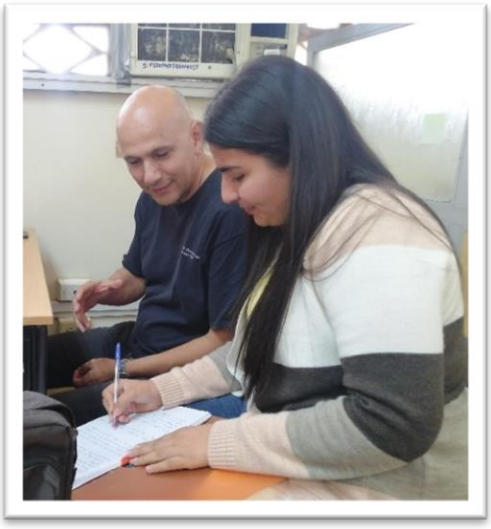
Profesional 2: las políticas y procedimiento a seguir por parte de la organización es establecer un reglamento al departamento de sistemas, llevar un control de los accesos realizados por parte de los usuarios y llevar un control de cambios contraseña casa dos meses.

Profesional 3: la recomendación es que se establezca contraseñas sólidas, establecer requisitos de complejidad y actualizaciones periódicamente, las contraseñas son las partes importantes para reducir el riesgo de acceso no autorizado; una política de control de acceso lo cual va a definir los derechos mínimos requeridos.

Profesional 4: se debe de establecer un plan de respuestas de incidentes, implementar monitoreo y detección de intrusos, realizar pruebas de penetración regulares también aprender de los incidentes, en mi parecer esto es lo se debería tomar en cuenta para proteger la seguridad y proteger los datos.

Figura 11

Entrevista Profesional 1



Nota. Fuente: La autora

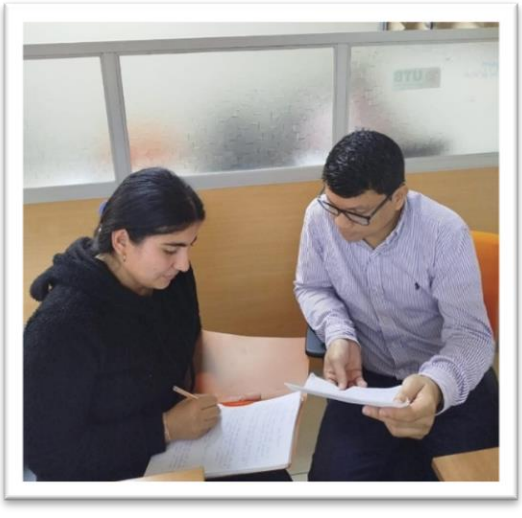
Figura 12

Entrevista Profesional 2

Nota. Fuente: La autora

Figura 13

Entrevista Profesional 3



Nota. Fuente: La autora

Figura 14

Entrevista Profesional 4

Nota. Fuente: La autora

INGENIERIA INTEGRASAYOX. S.A.

OF-CODE:: **2024-001-063**

Babahoyo, 7 de junio del 2024

Lcdo. Eduardo Galeas Guijarro

DECANO DE LA F.A.F.I

El presente es en atención y respuesta al Oficio: D-FAFI-UTB-00421-2024, con fecha de 5 de junio del 2024, relacionado con pasantías.

Estimado Decano, este documento le hace viable el acceso a nuestra infraestructura tecnologica, ademas de las consultas con nuestros expertos y demas información que requiera para elaborar su proyecto de titulación denominado: **"Análisis del sistema de soportes OSTicket en los aspectos de seguridad y protección de datos, en la empresa INGENIERIA INTREGRASAYOX S. A. ubicado en la ciudad de Babahoyo"**; la señorita **JAZMIN NOEMI CONTRERAS ANCHUNDIA**, con cedula: **120777082-5,** estudiante de Ingeniería en Sistemas de Información; proceso de titulación: ABRIL – AGOSTO 2024.

Particular que comunico para los fines pertinentes de titulación.

Atentamente,

Lcdo. Abel Monar E.
GERENTE GENERAL DE INGENIERIA INTEGRASAYOX. S.A.

RECIBIDO
UNIVERSIDAD TÉCNICA DE BABAHOYO
SECRETARIA FAFI
07-06-24 FECHA: 11:29. HORA:

CERTIFICADO DE ANÁLISIS
magister

COMPILATIO TRABAJO FINAL JAZMIN CONTRERAS

< 1%
Textos sospechosos

0% **Similitudes**
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% **Idiomas no reconocidos**
0% **Textos potencialmente generados por la IA**

Nombre del documento: COMPILATIO TRABAJO FINAL JAZMIN CONTRERAS.docx
ID del documento: fa4029b851d31384bcf41da3a885ae9b60fd182a
Tamaño del documento original: 1,85 MB

Depositante: DELGADO CUADRO ENRIQUE ISMAEL
Fecha de depósito: 5/8/2024
Tipo de carga: interface
fecha de fin de análisis: 5/8/2024

Número de palabras: 6170
Número de caracteres: 40.287

Ubicación de las similitudes en el documento: