LAS MEJORES PRÁCTICAS DE SEGURIDAD APLICADAS A NUESTRO SOFTWARE

La Seguridad para nosotros en helppeople hace parte de un ciclo vital en el desarrollo de nuestro software, donde garantizamos que todas nuestras aplicaciones sean robustas, soportadas y garantizadas por un alto nivel de seguridad.

A lo largo de la historia de helppeople, siempre nos hemos preocupado por la seguridad de nuestras aplicaciones, y ahora más que nunca cuando la tendencia en ataques cibernéticos ha ido aumentando.

Para nosotros la seguridad en nuestro software constituye una serie de pruebas que incluyen las diferentes fases de helppeople. Aplicamos las pruebas desde que proyectamos el producto, conceptualizamos el desarrollo, y finalmente en el código. Esto, en cada producto nuevo y actualización de los existentes.

Dejamos claro que, la seguridad del sistema como tal es una parte en lo que nos enfocamos, por ejemplo, contar con los protocolos SSL. Pero, también, abarcamos los componentes de seguridad que van inmersos en la arquitectura como la presencia de Firewalls. Sin embargo, estos dos conceptos no son suficientes para nuestro ciclo de seguridad, y por eso lo consideramos como una propiedad dinámica del software.

En helppeople, llamamos la seguridad como propiedad dinámica, porque pueden variar con el tiempo, y que constantemente pueden salir nuevas vulnerabilidades en el mundo digital y que pueden ser críticas. Es ahí, cuando nosotros como compañía contamos con diferentes mecanismos de control para identificar las vulnerabilidades a tiempo, trabajar en ellas y mantener la tranquilidad de que nuestros clientes no van a estar expuestos a algún ataque o caída del sistema.

Estudios de Amazon Web Service comprueban que el 50% de las vulnerabilidades tienen su origen en el diseño. Comúnmente los conocemos como “BUGS”, y pueden ser identificadas antes de salir a producción y solucionarlas antes de implementarla a los clientes. ¿Ya sabes entonces porqué en helppeople no sacamos versiones de prueba a los clientes?

Guía de desarrollo seguro

A continuación, te contaremos cual es nuestra guía de desarrollo seguro:

1. Nada es seguro, hasta que se demuestre lo contrario

En helppeople, no englobamos las funcionalidades sensibles con las no sensibles, ya que hay componentes confiables que pueden llegar a ser más vulnerables que otros. Entonces, identificamos cada una de las características de nuestras aplicaciones y las categorizamos por sensibles y no tan sensibles. A ambas se les hace pruebas, porque las NO sensibles también pueden ser foco de vulnerabilidad, hasta que no se demuestre lo contrario con verificaciones.

2. Creamos métodos de autenticación que sean difíciles de eludir.

Los métodos de verificación son los procesos que nos permiten comprobar la identidad de un usuario y asignarle un identificador único. Desarrollamos métodos de autenticación centralizados que cubra todas las posibles rutas de entrada, Esta práctica es uno de los pilares de la creación de aplicaciones seguras.

3. Permisos y aprobaciones, además de la verificación

Con los permisos o aprobaciones ratificamos si un usuario verificado puede realizar acciones que cambian el estado del sistema. El proceso de permisos o aprobaciones para la verificación de usuarios debe estar construido para evitar que la interacción llegue a manos malintencionadas.

4. Discernimos datos de instructivos de control

Separamos datos de instructivos de control cuando usamos lenguajes como JavaScript, ya que este puede reescribir su código o compilar el mismo en tiempo de ejecución, donde se reciben las mismas instrucciones como datos. Así bien, se vuelve primordial curar la entrada recibida por el sistema para evadir ataques donde manipulen los procesos de ejecución ingresando códigos maliciosos.

5. Validamos todos los datos explícitamente

Evaluamos todas las entradas del sistema y verificamos si deben seguir el concepto de listas blancas en lugar de listas negras, es decir, determinar lo que está permitido y rechazar todo el contenido no correspondiente. Debemos pensar que el atacante interpreta los datos como posibles lenguajes de programación con el objetivo de manipular el estado del sistema. Por lo tanto, verificamos estos datos de entrada y generamos un programa automático para convertirlos en una forma canónica conocida.

Incluso, esta verificación de entradas la realizamos cerca al momento en que los datos son en efecto utilizados, ya que el desfaje entre la verificación y el uso brinda una puerta de oportunidades para ciberataques.

Para poder echar a andar esto, construimos componentes sencillos que centralicen verificaciones tanto sintácticas –estructurales– como semánticas –de significado–, y sacamos el mayor provecho de los tipos de códigos presentes en el lenguaje de programación sobre el cual estamos trabajando.

6. Usamos criptografía correctamente

Entendemos las nociones criptográficas que aplican al sistema y en el desarrollo, es necesario para poder entender qué elementos y qué características de los mismos se buscan proteger, contra qué formas de ataque, y consecuentemente, cuál es la mejor manera en que logremos este objetivo.

Creamos nuestras propias soluciones criptográficas y acudimos a los mejores asesoramientos (AWS) con el fin de encontrar las mejores librerías y herramientas que nos permiten aumentar el costo de ataque para el ciber atacante.

7. Entendemos e Identificamos datos sensibles y cómo procedemos con su gestión

A veces resulta complicado mantener protegidos nuestros datos si no tenemos muy claro qué es lo que realmente buscamos cuidar. La definición de los datos cuya protección resulta fundamental para el funcionamiento del sistema es crítica, puesto que a partir de ella podremos comenzar a esbozar los procesos

para el diseño de la seguridad desde el mismo comienzo del ciclo de desarrollo, y no como un añadido en las etapas de implementación o despliegue.

8. Siempre tenemos en cuenta a los usuarios del sistema

Un sistema “perfecto” que no tiene en cuenta las necesidades de sus usuarios es un sistema inservible. La seguridad utilizable siempre es nuestra meta a alcanzar constantemente ya que en helppeople nos planteamos los objetivos de seguridad para el sistema. Por un lado, no es prudente transferir al usuario cuestiones de seguridad que pueden resolver los mismos desarrolladores, a fin de evitar la fatiga.

Por otro lado, mantenemos una comunicación con los usuarios para otorgar cierto grado de “transparencia” sobre cómo funciona nuestro sistema. Nuestra configuración por defecto es la configuración segura, siempre.

9. Integramos componentes para cambiar la superficie de ataque

Las aplicaciones actuales de helppeople constituyen sistemas complejos con muchos componentes interactuando de manera simultánea. Cada vez que se realiza un cambio en el sistema, el panorama de seguridad cambia y lo reevaluamos. Esta reexaminación es el resultado de la coordinación entre las áreas y proyectos.

Analizamos los componentes de manera unitaria y en equipo; teniendo en cuenta cómo se combinan, mantienen o reemplazan.

10. En helppeople consideramos cambios futuros en objetos y actores

Desde el diseño de nuestras herramientas, consideramos que las propiedades del sistema y sus usuarios cambian constantemente. Algunos factores que consideramos son el crecimiento de la población de usuarios, cómo las migraciones afectan al sistema, o cómo afectarán vulnerabilidades futuras sobre nuestras herramientas.

Nuestros procedimientos de actualización los realizamos de manera segura ya que los diseñamos con horizontes a futuros de corto, mediano o largo plazo.

11. Contamos con el mejor alineamiento estratégico de seguridad por AWS

En helppeople de la mano AWS velamos por la privacidad y seguridad de nuestros usuarios. Con AWS creamos en la infraestructura global más segura y sabemos que siempre nuestros datos y herramientas contaran con la mejor seguridad, incluida la capacidad para cifrarlos, trasladarlos y para gestionar la retención de estos. Todos nuestros datos que fluyen en la red global de AWS y que interconectan nuestros centros de datos y regiones se cifran de manera automática en la capa física antes dejar nuestras instalaciones protegidas. También, existen capas adicionales de cifrado.

Gracias a esto contamos con certificaciones de seguridad heredada por AWS como la certificación de conformidad con las normas ISO/IEC 27001:2013, 27017:2015, 27018:2019 e ISO/IEC 9001:2015 y CSA STAR CCM v3.0.1.

(https://aws.amazon.com/es/compliance/iso-certified/)

https://helppeoplecloud.com/wp-content/uploads/2021/09/Certificaciones-AWS.pdf

https://helppeoplecloud.com/wp-content/uploads/2021/09/csa_star_certification-1.pdf



Ya para terminar…

A lo largo de los años, como compañía en constante innovación nos mantenemos al margen de la seguridad, a entender y aceptar que la identificación y solución temprana de problemas posee un costo inversamente proporcional al tiempo que la vulnerabilidad permanece en nuestros sistemas.