Texto
Redacción Computing

ORIOL SOLÀ, CISO DE WEFOX

“Con los ataques controlados de Wise, los entornos de wefox ahora están más seguros”

wisesecurity GLOBAL

wefox

EL RETO

wefox, debido a su gran dependencia de su exposición digital y su compromiso con la mejora continua, quiere someter sus sistemas principales a una auditoría de Ethical Hacking and Vulnerability Assessments. Para ello confía en Wise Security Global.

Wefox es la aseguradora digital número uno de Europa. Se fundó con una gran visión en mente: simplificar los seguros. Cuenta con la confianza de clientes en cinco países (8 oficinas en Europa, más de 600 empleados, más de 1.000 asesores).

La compañía utiliza la tecnología para simplificar los seguros. “Una mejor tecnología significa que somos más eficientes, por lo que ahorramos dinero, que le pasamos a nuestro cliente. Hacemos menos preguntas y facilitamos el seguro, para que pueda dedicar tiempo a pensar en otras cosas”, explica Oriol Solà, CISO de wefox.

La empresa aseguradora, debido a su gran dependencia de su exposición digital y su compromiso con la mejora continua, ha querido someter sus sistemas principales a una auditoría de Ethical Hacking and Vulnerability Assessments. Para ello han confiado en Wise Security Global.

Oriol Solà explica a Computing su caso de éxito gracias a este proyecto conjunto con Wise Security Global.

¿Cuáles eran los retos que wefox tenía por delante para mejorar su ciberseguridad?

El principal reto para nuestra compañía es una constante: Proteger las plataformas web de las amenazas de ciberseguridad que pueden provocar tiempo de inactividad o degradación empresarial.

También debemos garantizar los máximos estándares de seguridad para evitar cualquier fuga de datos de nuestros clientes.

Cualquier proyecto de ciberseguridad en wefox tiene en el centro de la diana generar confianza digital en nuestros clientes, y para ello debemos revisar y optimizar las operaciones actuales, y sensibilizar y empoderar a la organización en materia de ciberseguridad.

En este caso, ¿en qué os ha ayudado Wise Security Global?

Wise Security Global, con quien llevamos una sólida trayectoria de colaboración, ha centrado sus esfuerzos en 2 frentes para cumplir los objetivos de wefox:

- Ethical Hacking
- Protección perimetral, vigilancia y respuesta a incidentes críticos

Es muy esclarecedor exponernos al ataque controlado de un tercero para hacer autocríticas y ver dónde somos más débiles. Los ciberataques evolucionan y nuestros sistemas deben ser revisados continuamente para que sean lo más seguros posible.

¿Cuál ha sido la hoja de ruta para ello?

Para mejorar el nivel de madurez de wefox, Wise nos propuso acciones específicas desde su área de EHVA (Ethical Hacking and Vulnerability Assessments). En concreto, auditoría de seguridad de apps, de aplicaciones web, pentesting de vulnerabilidades, así como la identificación de errores de configuración o vulnerabilidades en la web.

¿Da vértigo descubrir hasta dónde puede acceder un ciberataque cuando no está controlado?

Sí, por eso es mucho mejor prevenir y hacer esa autocrítica, y que un tercero como Wise trate de colarse hasta dentro para solucionar cuanto antes esas posibles brechas de seguridad. Las acciones de pentesting ponen a prueba los sistemas de la organización de manera interna y externa para refortalecerlos.

¿Una acción de pentesting remueve las tripas de su equipo?

Nos activa todavía más la conciencia de las verdaderas vulnerabilidades, entrena a nuestro equipo en tiempo real y pone a prueba la habilidad del equipo para reaccionar frente ataques específicos.

Aclara la percepción de la empresa sobre el estado actual de los sistemas, y ayuda a priorizar las inversiones en seguridad. Y, sobre todo, permite a wefox la oportunidad de actuar con antelación y corregir las brechas de nuestra infraestructura antes de un ataque.

¿El resultado de una acción de pentesting podría tomarse como una foto de tareas mal resueltas?

Al contrario. Nadie está a salvo de un ciberataque y cuanto más preparado estás, mejor. Por eso, preocuparnos por saber dónde tenemos puntos más débiles y solucionarlos antes de tener un problema real, mejora la lealtad e imagen de nuestra marca. El pentesting nos da una oportunidad para reafirmar nuestro compromiso con la seguridad e inspirar confianza en nuestros clientes.

Además, los proyectos de Ethical Hacking que llevamos a cabo con los expertos de Wise nos ayudan a cumplir con la regulación de protección de datos y mitigar las sanciones de pérdida de información, en un sector tan sensible como el asegurador.

¿Qué otros beneficios conllevan someterse a una auditoría de Ethical Hacking?

Las acciones de pentesting reducen costes asociados a tiempos de inactividad provocados por incidentes de ciberseguridad. Además, el equipo de Wise nos ha ayudado a implantar el modelo de responsabilidad compartida de la ciberseguridad. Esto es: no solo yo como CISO y el resto de mi equipo somos responsables de la seguridad de wefox, también nuestros proveedores de sistemas, entornos y apps deben implicarse y ser partícipes de la resolución de vulnerabilidades detectadas. ■

EL PLAN DE ACCIÓN

Wise implanta en wefox un proceso de pentesting y auditoría de seguridad en todas las apps, y aplicaciones web de la compañía de seguros.

LOS BENEFICIOS

- Las acciones de pentesting ponen a prueba los sistemas de la organización para refortalecerlos.
- Activa la conciencia de las verdaderas vulnerabilidades y ayuda a priorizar las inversiones en seguridad.
- Permite a wefox actuar con antelación y corregir las brechas de su infraestructura antes de un ataque.
- Entrena a su equipo en tiempo real.
- Mejora la lealtad e imagen de su marca. El pentesting reafirma su compromiso con la seguridad e inspira confianza en sus clientes.
- Ayuda a cumplir con la regulación de protección de datos y mitigar las sanciones.
- Las acciones de pentesting reducen costes asociados a tiempos de inactividad provocados por incidentes de ciberseguridad.