ESTUDIO DE CASO

PROGRAMA PÚBLICO DE BUG BOUNTY

BLABLACAR

Enero 2020

YES WE HACK

BlaBlaCar

¿Qué le ha decidido a poner en marcha un programa de Bug Bounty?

Alain Tiemblo, Ingeniero jefe de seguridad web, BlaBlaCar:
En el pasado, solíamos recurrir a auditorías convencionales: escaneos de vulnerabilidades, pentests, análisis de código, -etc. Esto nos permitió aclarar ya muchas cosas.
Más tarde, empezamos a recibir mensajes de troles en las redes sociales, señalando posibles fallos, sin avisos ni detalles... También recibimos correos electrónicos en atención al cliente indicando vulnerabilidades, pero también en este caso sin ninguna información detallada o útil. La pretensión de estas personas era que se les pagara antes de facilitar más datos, pero, a falta de pruebas de fallos contrastados, no nos era posible remunerarles.

Estos mensajes se hicieron cada vez más frecuentes, **hasta el punto de animarnos a pasar al Bug Bounty, para dar sentido a estas comunicaciones.**

Realizamos un estudio comparativo de las diferentes plataformas de Bug Bounty en Europa y **nos decantamos por YesWeHack, principalmente por razones normativas y de titularidad de los datos.** Un segundo criterio fue la cantidad de hackers activos en dicha plataforma: de poco sirve poner dinero y energía en un programa de Bug Bounty si no hay una masa crítica de hackers para buscar fallos en los sistemas informáticos de manera efectiva.

Paralelamente, incorporamos el archivo security.txt a nuestro sitio web para dirigir a los hackers hacia la plataforma YesWeHack, al ser el Bug Bounty una buena forma de promover la comunicación coordinada de vulnerabilidades (CVD, por sus siglas en inglés: Coordinated Vulnerability Disclosure).

¿Podría describirnos la evolución y el desarrollo de su programa desde el principio?

Alain Tiemblo :
Pusimos en marcha nuestro programa de forma privada a finales de 2017, con una fase de rodaje bastante importante: nada más hacerlo público se recibieron muchos informes, pero luego perfeccionamos gradualmente nuestro programa: definimos mejor nuestros perímetros, el tipo de vulnerabilidades que nos interesaba detectar, etc. Desde el principio, recibimos fallos «reales», potencialmente críticos, lo que nos convenció de la pertinencia del modelo y de la eficacia de la plataforma.

Después de una semana, el número de fallos empezó a disminuir, pero **las comunicaciones eran cada vez más interesantes, ya que los hackers «entraban» en nuestro producto y elaboraban informes realmente específicos para nuestra organización.**

Al cabo del primer mes, la situación se tranquilizó mucho. Seguidamente, invitamos a hackers nuevos para contar con otros puntos de vista y opiniones profesionales sobre ciertos aspectos específicos de nuestro programa.
El programa privado también permitió a nuestros equipos aprender a gestionar los informes, a clasificarlos y calificarlos, así como ajustar las reglas.
Después de esta fase de rodaje, decidimos hacer público el programa en abril de 2018, es decir, siete meses después del inicio en privado de nuestro programa.

Estábamos realmente satisfechos con la calidad de los intercambios con los hackers durante la fase privada, por lo que no nos preocupaba pasar a una versión pública... ¡Simplemente queríamos más hackers en nuestro programa!
Asimismo, había un mensaje importante que deseábamos lanzar: ¡cualquiera que encuentre un fallo puede comunicarlo! Naturalmente, tras hacer público el programa recibimos más informes, pero dentro de unos parámetros totalmente manejables.

Hoy nos esforzamos por obtener informes de calidad y sobre todo fallos cada vez más complejos que requieren mayor dedicación y pericia a los hackers.

En este contexto, hemos aumentado el importe de nuestras recompensas por vulnerabilidades críticas. El reto es, con la ayuda de YesWeHack, atraer a investigadores que encuentren cosas interesantes sin desbaratar nuestro presupuesto de recompensas.

A su juicio, ¿qué ventajas tiene el Bug Bounty frente a soluciones tradicionales como el pentest?

Antonin Le Faucheux – CISO – BlaBlaCar:
En mi opinión, cada herramienta tiene su utilidad. **La ventaja del Bug Bounty es, en primer lugar, el crowdsourcing:** cuando contratas una empresade auditoría, tienes varios consultores disponibles, mientras que con el Bug Bounty, tenemos potencialmente cientos o miles de expertos trabajando en nuestro sitio web.

Otra consideración es **la continuidad, el 365/24/7,** mientras que un pentest suele desarrollarse durante un periodo limitado y aporta una visión del estado de las cosas en un punto del tiempo concreto. **Esta continuidad es esencial para detectar bugs lo antes posible, cuando hacemos actualizaciones muy frecuentes de nuestras aplicaciones.**

Otro rasgo diferenciador es que el Bug Bounty genera una obligación de resultado, mientras que el pentest solo entraña una obligación de medios. Este punto es igualmente interesante para nuestra comunicación interna con nuestros equipos: podemos decirles que solo estamos pagando a personas que encuentran vulnerabilidades explotables, en lugar de pagarles «para ver» si encuentran algo, sin esta obligación de obtener resultados.

El Bug Bounty también lanza un mensaje claro a los hackers. Durante mucho tiempo, un gran número de empresas amenazó con demandar judicialmente a los hackers que les comunicaban fallos. Como resultado, se sembró cierto temor entre ciertos hackers que detectaban fallos, que dudaban si ponerse en contacto con las empresas afectadas por miedo a represalias.

Con nuestro programa de Bug Bounty lanzamos un mensaje muy claro a la comunidad: nuestro deseo es que nos comuniquéis los fallos y, a dicho efecto, os ofrecemos un marco legal y seguro, con la intervención de intermediario de confianza entre nosotros para que todo se desarrolle correctamente.

Este mensaje es muy importante para nosotros, porque queremos que los hackers se digan: «he encontrado una vulnerabilidad en BlaBlaCar, puedo obtener una remuneración por este trabajo de manera legal y sin correr riesgos». En lugar de que algunos terminen acudiendo al mercado negro para vender este fallo.

¿Qué tratamiento interno dan ustedes a estos informes?

Antonin Le Faucheux:
Somos varios los que nos encargamos de gestionar el programa Bug Bounty y de recibir informes de vulnerabilidades.El equipo de seguridad se encarga de darles curso, hace un primer examen para determinar la gravedad del bug y decide si es preciso actuar de inmediato, o no. Si el fallo resulta ser complejo, se aborda en equipo.

Una vez que la vulnerabilidad ha sido calificada internamente, se notifica al equipo en cuestión a través de una herramienta de ticketing proporcionada por la plataforma YesWeHack.

Esta herramienta de ticketing nos permite realizar un seguimiento del avance de los equipos en sus procesos de corrección y reactivarlos si fuera necesario.
A continuación, se pasa a la fase de verificación de la corrección con la ayuda del hunter. A menudo esto no es más que una formalidad, ya que, por lo general, la hemos comprobado nosotros mismos, pero siempre es interesante contar una opinión externa y a veces hay sorpresas: el hunter nos indica lo que no se ha corregido correctamente.

¿Ha percibido cambios dentro de sus equipos desde que lanzaron el Bug Bounty?

Ahora se tiene mucho más en cuenta el aspecto de la seguridad. **En nuestras formaciones internas ya no se habla de fallos posibles, sino que se muestran casos concretos, vulnerabilidades comunicadas en el marco de nuestro programa, lo que tiene un impacto mucho mayor.**

¿Cómo encaja el Bounty Bug en su política de agilidad?

Antonin Le Faucheux:
El Bug Bounty se integra en el flujo de trabajo de los equipos a través de la herramienta de ticketing. **La idea es que los fallos de seguridad sean tareas como los demás,** que se delegarán en los equipos competentes con el nivel de prioridad pertinente.
Al tratarse de un proceso continuado, la posibilidad de ampliar los perímetros de nuestro programa con un clic nos permite detectar cosas rápidamente en estos nuevos perímetros, lo que nos hace más ágiles: nada más actualizar una aplicación, podemos ponerla a prueba, tener en cuenta los resultados y configurar fácilmente un bucle de retroalimentación.

¿Cuál será la próxima fase de su estrategia de Bug Bounty?

La próxima fase del Bug Bounty es seguir perfeccionando nuestro programa para mejorar constantemente la calidad de la relación con nuestros colaboradores y clientes, atraer a los mejores hackers, etc.