YES WE HACK

yousign

YOUSIGN

Programa Privado de *Bug Bounty*

ESTUDIO DE CASO

¿QUÉ LES LLEVÓ A OPTAR POR EL *BUG BOUNTY*?

KEVIN DUBOURG, DIRECTOR DE PROGRAMAS DE *BUG BOUNTY*, YOUSIGN:

Hay unas cuantas plataformas de este tipo, la mayoría con sede en Estados Unidos. Nosotros les pedíamos a los *hunters* invitados a nuestros programas que cumplieran ciertas garantías y YesWeHack ofrecía dichas garantías junto con la confianza para poner en marcha un programa de *bug bounty*.

A SU JUICIO, ¿QUÉ VENTAJAS TIENE EL *BUG BOUNTY* FRENTE A SOLUCIONES TRADICIONALES DE CIBERSEGURIDAD, COMO LOS TEST DE PENETRACIÓN?

KEVIN DUBOURG, DIRECTOR DE PROGRAMAS DE *BUG BOUNTY*, YOUSIGN:

Ofrece diversidad en términos de perspectivas y aptitudes. Cada *hunter* tiene su propio enfoque, su manera de hacer las cosas: un enfoque único que genera un ataque particular. Es algo que se diferencia de los test de penetración y supone un reto mucho más duro. Con el *bug bounty*, dejamos atrás el mundo de los test de penetración en aras de disfrutar de 10, 20 o 30 visiones diferentes y desafiar realmente a nuestros equipos de trabajo.

Es también de reseñar que no todos los *hunters* son necesariamente "profesionales de la ciberseguridad". En este mundillo hay todo tipo de gente y, así, podemos elegir en función de la nacionalidad, las habilidades o la clasificación en la plataforma.

Sin embargo, el principal valor del *bug bounty* son la continuidad y la recurrencia de los test a lo largo del año: en cuanto lanzamos una nueva versión, integramos el programa existente y recibimos inmediatamente información acerca de la seguridad de la nueva versión. No hay que esperar un año para hacer el siguiente test de penetración y poder comprobar la seguridad de la actualización. Este enfoque está integrado dentro del ciclo de vida de nuestro proyecto.

Nuestro campo de acción evoluciona de forma constante y los fallos evolucionan en paralelo. Los fallos de seguridad ocurren todos los días, no solo una vez al año, y el *bug bounty* nos permite detectarlos y darles solución a tiempo. Nos permite supervisar nuestros servicios casi constantemente, algo que resulta muy tranquilizador. Tampoco sería posible, desde el punto de vista económico, realizar un test de penetración a cada implementación, aunque fuera necesario.

La rentabilidad de la inversión resulta convincente también. Yousign lleva a cabo un test de penetración cada año. Algo que sale bastante caro en comparación con un programa de *bug bounty*. Resulta un tanto demencial si se piensa bien: cuestan más o menos lo mismo, pero el *bug bounty* abarca todo un año, mientras que una auditoría únicamente dura una semana.

yousign

¿SUPONE EL *BUG BOUNTY* EL FINAL DE LOS *PENTEST* O ES ALGO COMPLEMENTARIO?

KEVIN DUBOURG, DIRECTOR DE PROGRAMAS DE *BUG BOUNTY*, YOUSIGN:

Para Yousign ambos elementos continuarán siendo complementarios. Podría significar el final de los test de penetración en algunos sectores, pero no en el nuestro: como prestador de confianza a terceros, estamos obligados a realizar auditorías periódicas. En un entorno regulatorio menos estricto, probablemente yo consideraría utilizar únicamente el *bug bounty*.

No obstante, el *bug bounty* es muy importante para nuestras operaciones de ventas y de *marketing*: es claramente un elemento diferenciador para grandes cuentas potenciales. Lo mencionamos sistemáticamente en nuestros formularios de solicitud de propuestas, ya que en el mercado se lo considera como un sello distintivo de calidad.

¿CÓMO SE COMPARAN LOS RESULTADOS ENTRE LOS TEST DE PENETRACIÓN Y EL *BUG BOUNTY*?

KEVIN DUBOURG, DIRECTOR DE PROGRAMAS DE *BUG BOUNTY*, YOUSIGN:

He encargado la misma cantidad de informes de uno y otro pero el *bug bounty* genera muchos más resultados que los test de penetración. Es más, después de haber llevado a cabo un test de penetración en un área determinada, realizar el *bug bounty* siempre aporta vulnerabilidades adicionales.

Uno de los problemas asociados con los test de penetración es que los resultados dependen principalmente de la experiencia de quien los hace. Nuestro último test de penetración puso de manifiesto algunas cosas relevantes, pero cuando se comparan los resultados con los del programa de *bug bounty* que aplicamos después, no había parangón.

> **“Después de haber llevado a cabo un test de penetración en un área determinada, realizar el *bug bounty* siempre aporta vulnerabilidades adicionales.**

¿HA OBSERVADO ALGÚN CAMBIO EN SUS EQUIPOS DE TRABAJO DESDE QUE UTILIZAN EL *BUG BOUNTY*?

KEVIN DUBOURG, DIRECTOR DE PROGRAMAS DE *BUG BOUNTY*, YOUSIGN:

Sí, desde luego. Al principio yo administraba los programas por mi cuenta, pero poco después involucré a los equipos de desarrollo para que pudieran gestionar procesos como la respuesta directa a los *hunters* y la corrección de fallos. La mayoría de los informes afectaban al equipo de aplicaciones, que tuvo que aceptar los resultados y sacar las cosas adelante.

Es más, rápidamente vimos que las interacciones con los *hunters* influían en sus métodos de entrega y de trabajo: no sólo integraban la seguridad en su labor de desarrollo de forma más eficaz, sino que también empezaban a "pensar" de forma diferente, con la mente siempre puesta en los aspectos de seguridad. Se podría decir que no sólo cumplen con los clientes, sino también con los *hunters*.

¿CUÁLES SERÁN LOS SIGUIENTES PASOS?

KEVIN DUBOURG, DIRECTOR DE PROGRAMAS DE *BUG BOUNTY*, YOUSIGN:

El siguiente paso es ampliar el uso del *bug bounty*. Además de los programas actuales en nuestros entornos de producción y despliegue, queremos integrar el *bug bounty* dentro de nuestro flujo de trabajo de integración y entrega continua (CI/CD) para que complementen nuestra batería de test funcionales y de unidades. Es algo que debe hacernos todavía más ágiles. El *bug bounty* es ciertamente un componente clave de nuestro enfoque en integración/entrega continua.

Con el tiempo, es posible que pasemos a un programa público.

SOBRE

YES WE HACK

Fundada en 2015, YesWeHack es una plataforma mundial de *Bug Bounty* & VDP.

YesWeHack ofrece a las empresas un enfoque innovador de la ciberseguridad con *Bug Bounty* (pago por vulnerabilidad descubierto), conectando a más de 25.000 expertos en ciberseguridad (*hackers* éticos) de 170 países con organizaciones, para asegurar sus perimetros expuestos e informar de las vulnerabilidades de sus sitios web, aplicaciones móviles, infraestructura y dispositivos conectados.

YesWeHack gestiona programas privados (sólo por invitación) y programas públicos para cientos de organizaciones en todo el mundo en cumplimiento de las más estrictas regulaciones europeas.

Además de su plataforma de *Bug Bounty*, YesWeHack también ofrece: apoyo para la creación de una Política de Divulgación de la Vulnerabilidad (VDP), una plataforma de aprendizaje para *hackers* éticos llamada Dojo y una plataforma de capacitación para instituciones educativas, YesWeHackEDU.

⟶ CONTÁCTENOS

⟶ VISITE NUESTRO SITIO WEB

yousign