GRUPO EUROPEO DE SEGUROS

Programa privado de Bug Bounty

ESTUDIO DE CASO

¿PODRÍA PRESENTARSE BREVEMENTE?

Soy el CISO de uno de los mayores grupos de seguros europeos. Mi equipo quería sobre todo levantar un "escudo cibernético" para proteger al Grupo y a todas sus filiales, ofreciendo varios servicios de seguridad a nuestras filiales, incluido el Bug Bounty.

¿QUÉ LES LLEVÓ A PONER EN MARCHA UN PROGRAMA DE BUG BOUNTY?

Descubrí este modelo hablando con varios CISOs de grandes instituciones francesas. Las recomendaciones de instituciones financieras tan exigentes en materia de seguridad obviamente influyeron en mi decisión. Primero realizamos algunas pruebas que resultaron ser concluyentes, por lo que pusimos gradualmente en marcha varios programas de Bug Bounty. Se trata de un enfoque diferente al que es preciso acostumbrarse.

YES WE HACK

A SU JUICIO, ¿QUÉ VENTAJAS TIENE EL BUG BOUNTY FRENTE A SOLUCIONES TRADICIONALES DE CIBERSEGURIDAD?

En primer lugar, garantiza una vigilancia continuada, no solo puntual, como ocurre con las pruebas de intrusión convencionales.

Si hago un pentest de dos semanas al año, eso significa que nos quedamos "sin protección" durante las otras 50 semanas, lo cual parece inadmisible hoy día.

En este sentido, las pruebas automatizadas pueden ser también muy útiles, pero menos concluyentes.

Ahora, junto con el Bug Bounty, tengo investigadores que trabajan permanentemente en mis perímetros.

Esta continuidad de los test es primordial, sobre todo cuando hay que hacer entregas frecuentes en un contexto de desarrollo cada vez más ágil.

El Bug Bounty también nos permite ser más flexibles: se pueden poner a prueba entornos aún en desarrollo, en fase de aceptación, antes de la puesta en producción, según el ritmo de cada proyecto, algo difícil de hacer en el marco de los pentest habituales.

La plataforma YesWeHack nos permite ajustar nuestras reglas de cada programa, incluido el sistema de recompensas, en función de la fase del proyecto.

También mencionaría la capacidad de respuesta y la disponibilidad. Es cada vez más difícil, y a veces imposible, encontrar buenos pentesters justo cuando más se les necesita, es decir, cuando se hace una nueva versión.

> **"Con el Bug Bounty, se pulsa el botón y arranca, pueden iniciarse pruebas en cualquier momento y obtener la confirmación del parche muy rápidamente.**

Con el Bug Bounty, se pulsa el botón y arranca, pueden iniciarse pruebas en cualquier momento y obtener la confirmación del parche muy rápidamente.

Por último, un valor añadido adicional radica en la variedad de vulnerabilidades reportadas.

Se ven escenarios más interesantes donde, por ejemplo, los investigadores han encontrado trazas de vulnerabilidad que, combinadas, permitirían ataques inéditos. Se trata de vulnerabilidades que hasta ahora no se atajaban, por no tener conocimiento de ellas, y que hemos podido corregir en profundidad.

Con el Bug Bounty, realmente te metes en la mente de un hacker más que en la fría vulnerabilidad encontrada en el resultado de una auditoría.

¿SUPONE EL BUG BOUNTY EL FINAL DEL PENTEST O ES ALGO COMPLEMENTARIO?

En mi opinión, es complementario. Pero la realidad es que, dado el número de pruebas que hay que realizar, la disponibilidad de las firmas de auditoría no es suficiente...

De ahí el carácter indispensable del Bug Bounty. Además, las auditorías de pentest, aparte de lo ya mencionado, tienen límites: hay que programarlas con mucha antelación, prever una fecha de inicio y otra de finalización, encargarse de la gestión del proyecto, etc.

Esta sincronización es un auténtico quebradero de cabeza, sobre todo en un entorno de desarrollos ágiles. Si alguna vez una entrega se retrasa dos días en un perímetro, los pentesters dejan de estar disponibles, lo que plantea un serio problema de administración.

Algo que también me gusta mucho en el Bug Bounty es la contrauditoría. En las auditorías tradicionales de pentest casi nunca hay contrauditoría. Tras un pentest, un desarrollador de mi equipo puede decirme "he corregido el fallo", pero normalmente solo tengo su promesa.

El Bug Bounty me permite delegar este control en el investigador, que es totalmente objetivo. Esto me permite corregir una vulnerabilidad y confirmar la corrección sobre la marcha, a diferencia de una contrauditoría tradicional, que no podría poner en marcha hasta después de haber solucionado todas mis vulnerabilidades.

Ahora, cuando se descubre una vulnerabilidad grave o crítica, sé que se corregirá rápidamente y que podré dormir tranquilo. (Risas)

YES WE HACK

¿HA PERCIBIDO CAMBIOS EN SUS EQUIPOS DESDE LA PUESTA EN MARCHA DEL PROGRAMA DE BUG BOUNTY?

Hay más comunicación, sin duda alguna, pero el punto principal que observo es la aceleración del ritmo de corrección: nuestros desarrolladores corrigen mucho más deprisa. Responder a los investigadores, pagarles, cerrar los informes, etc., lleva a los desarrolladores a reaccionar con mayor rapidez, lo que redunda en un acortamiento muy notable de los plazos de corrección.

¿QUÉ HAY DE LA AGILIDAD?

Como he dicho anteriormente, hemos creado programas dedicados a probar los entornos antes de su puesta en producción. Por lo tanto, detectamos y corregimos las vulnerabilidades cada vez más en las fases iniciales de los proyectos, lo que permite 1. formar a nuestros desarrolladores "sobre la marcha" y 2. acelerar nuestras entregas, ya que hay muchas menos correcciones que hacer en las fases de aceptación y en producción.

Así pues, estamos ganando en capacidad de respuesta, lo que redunda tanto en el interés de los desarrolladores como de la empresa.

¿CUÁLES SERÁN LOS SIGUIENTES PASOS?

La primera etapa consistió en ampliar gradualmente los perímetros del Grupo. Y en estos perímetros, para pasar gradualmente de la caja negra a la caja gris.

La segunda etapa, en la que estamos actualmente, es poner el servicio a disposición de nuestras filiales, ofreciéndoles algo nuevo y con visión de futuro, que les permita renovar su visión de la ciberseguridad y de las auditorías.

"Estamos ganando en capacidad de respuesta, lo que redunda tanto en el interés de los desarrolladores como de la empresa.

SOBRE

YES WE HACK

Fundada en 2013, 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 23 000 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