GROUPE ADP

Programa Público de *Bug Bounty*

ESTUDIO DE CASO

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

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

El equipo que se encarga de la seguridad del grupo llevó la iniciativa en este proyecto. Yo no tenía ninguna experiencia previa en *bug bounty*, pero muy rápidamente vimos las ventajas y la potencia de este modelo. Y aunque de entrada no tenía dudas ni preocupaciones específicas, ahora todo lo que veo son ventajas. Los *bugs* detectados por los *hunters* son vulnerabilidades que nosotros y nuestros auditores no hubiéramos visto de otra forma, y que lógicamente podrían aprovechar los malos.

ERIC VAUTIER, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, GROUPE ADP:

En ciberseguridad la anticipación lo es todo. Tienes que estar un paso por delante de los *hackers*. Por ello, hay que seguir de cerca las innovaciones del mercado. En el mundo digital, protegerse "a la antigua" supone sin duda quedarse a la zaga. Y una buena forma de ponerse al día es trabajar directamente con investigadores en materia de seguridad que utilizan los métodos de los *hackers* y piensan como ellos.

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

Hoy en día el *bug bounty* es uno de los pilares de nuestra estrategia de seguridad de la web. Por supuesto, es vital establecer las reglas de los programas con cuidado: hay que estructurar los test de forma correcta, para que los *hunters* no "dispersen" sus esfuerzos. Hay que identificar los "límites" adecuados y, en este punto, la configuración del programa es esencial. Empezamos con un perímetro bien delimitado y lo ampliamos sobre la marcha.

"Y una buena forma de ponerse al día es trabajar directamente con investigadores en materia de seguridad que utilizan los métodos de los *hackers* y piensan como ellos.

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

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

Las pruebas continuas, esa es la gran fortaleza del *bug bounty*. Los test de penetración se realizan en un momento determinado, no después de cada pequeña entrega. En cambio, tenemos *hunters* que trabajan de forma continuada con el *bug bounty*. Están atentos a cualquier novedad, con lo cual pueden detectar si cualquier cambio genera posibles vulnerabilidades.

ERIC VAUTIER, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, GROUPE ADP:

En un mundo perfecto deberíamos testar sistemáticamente cada actualización de nuestro sitio web. Esto implicaría realizar un test de penetración cada semana, o incluso más a menudo... y todo el mundo sabe que eso no es factible. El *bug bounty* hace que esa verificación continua sea algo posible.

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

Me llegan informes que no recibía con nuestros test de penetración. Esos informes son también mucho más granulares, particularmente en cuanto a la experiencia de navegación en el sitio web. Los auditores no tienen necesariamente ese enfoque. Es más, un test de penetración tiene un plazo limitado, mientras que los *hunters* se toman el tiempo necesario para llegar lo más lejos posible. A medida que pasa el tiempo, se van familiarizando cada vez más con nuestros perímetros, de modo que pueden profundizar aún más.

ERIC VAUTIER, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, GROUPE ADP:

Un programa de *bug bounty* también puede utilizarse para informar de vulnerabilidades de aplicaciones más funcionales, no solo técnicas. Para mí, eso es lo que lo diferencia genuinamente de los test de penetración. Se trata de un enfoque completamente diferente. Un test de penetración en muchas ocasiones se basa en herramientas automatizadas, mientras que el *bug bounty* se basa en esas herramientas con un enfoque más humano.

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

La interacción con los *hunters* resulta también interesante. Nos explican las vulnerabilidades que han encontrado y cómo solucionarlas de forma eficaz. Así podemos aprovechar su experiencia.

Desde luego, el *bug bounty* exige cierta inversión. Hay que estar dispuesto a entender qué es lo que los hunters han intentado hacer, hablar con ellos... Y nos obligan a plantearnos nuevas preguntas: ¿cómo podría un maleante eludir nuestras medidas de protección?

GROUPE ADP

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

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

Para mí, una cosa no funciona sin la otra. Por una parte, no estamos probando necesariamente lo mismo con ambos métodos. Por otra, no podemos aventurarnos en lo desconocido sin tener un nivel mínimo de certidumbre por anticipado. El *bug bounty* llega en una etapa más madura del desarrollo lógico de los acontecimientos. Hay que aprovechar un nivel de base mínimo de seguridad antes de poner en marcha el *bug bounty*. Dicho esto, con el alcance actual, los test de penetración ya no son necesarios. El *bug bounty* es suficiente por sí solo. Hay que poner el listón en el nivel adecuado al principio, y luego se convierte en un proceso recurrente.

> **"Dicho esto, con el alcance actual, los test de penetración ya no son necesarios. El *bug bounty* es suficiente por sí solo.**

¿CÓMO ENCAJA EL *BUG BOUNTY* EN SU POLÍTICA DE AGILIDAD?

DANIEL DIEZ, JEFE DE LA DIVISIÓN DE FÁBRICA DIGITAL, GROUPE ADP:

Como todo el mundo, tenemos herramientas para gestionar recursos, construcciones, proyectos y analíticas de rendimiento. También utilizamos herramientas para registrar y hacer un seguimiento de cada nuevo informe de vulnerabilidades desde el programa de *bug bounty*. En cada etapa verificamos qué datos relevantes podemos incluir, a fin de dar respuesta a las incidencias según se vayan presentando.

¿QUÉ LES HA MOVIDO A DARLE UN CARÁCTER PÚBLICO? ¿CÓMO HA CAMBIADO SU ENFOQUE CON EL *BUG BOUNTY*?

ERIC VAUTIER, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, GROUPE ADP:

La principal ventaja es maximizar nuestra cobertura de riesgos mediante la multiplicación del número de test potenciales. También nos permite disponer de un canal único para informar de vulnerabilidades en nuestro sitio web.

¿CUÁLES SERÁN LOS SIGUIENTES PASOS?

ERIC VAUTIER, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, GROUPE ADP:

Vamos a abrir nuevas áreas de aplicación, en otras aplicaciones y con otras entidades empresariales que utilizan el mismo modelo: inicialmente un programa privado que luego tendrá carácter público.

SOBRE

YES WE H/CK

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

GROUPE ADP