YES WE H/CK

BlaBlaCar

BLABLACAR

Programme de Bug Bounty public

ÉTUDE DE CAS

YES WE HACK

QU'EST-CE QUI VOUS A DÉCIDÉ À LANCER UN PROGRAMME DE BUG BOUNTY ?

ALAIN TIEMBLO, WEB SECURITY LEAD ENGINEER, BLABLACAR :

Auparavant, nous faisions appel à des audits classiques : scans de vulnérabilités, pentests, analyse de code, etc. Cela nous a déjà permis de dégrossir pas mal de choses.

Puis, on a commencé à recevoir quelques messages de trolls sur les réseaux sociaux, signalant des failles potentielles, sans préavis et sans aucun détail... On a aussi reçu quelques e-mails via le support client concernant des vulnérabilités, mais là encore, sans information précise ni exploitable. Ces personnes souhaitaient se faire payer avant d'en dire plus, mais en l'absence de preuve d'une faille avérée, il nous était impossible de les rémunérer.

Ces messages se sont faits de plus en plus nombreux, jusqu'au point où nous avons décidé de franchir le pas du Bug Bounty, afin de cadrer ces remontées.

Nous avons fait un comparatif des différentes plateformes de Bug Bounty en Europe et nous avons choisi YesWeHack principalement pour des raisons de régulations et de souveraineté des données. Le second critère était le nombre de hunters actifs sur la plateforme : ça ne sert pas à grand-chose de mettre de l'argent et de l'énergie dans un programme de Bug Bounty s'il n'y a pas une masse importante de hunters pour chercher efficacement des failles.

Nous avons en même temps intégré le security.txt sur notre site pour orienter les hunters vers la plateforme YesWeHack, le Bug Bounty étant une bonne façon d'inciter la remontée coordonnée de vulnérabilités (CVD en anglais).

POUVEZ-VOUS NOUS DÉCRIRE L'ÉVOLUTION ET LE DÉROULEMENT DE VOTRE PROGRAMME DEPUIS LE DÉBUT ?

ALAIN TIEMBLO :

Nous avons débuté en programme privé fin 2017, avec une phase de rodage assez importante. Quand on a ouvert, on a d'abord reçu beaucoup de rapports, puis nous avons progressivement affiné notre programme : on a mieux défini nos périmètres, le type de vulnérabilités qu'on souhaitait voir remontées, etc. Dès le début on a reçu de « vraies » failles, potentiellement critiques, ce qui nous a convaincu de la pertinence du modèle et de l'efficacité de la plateforme. Après une semaine, le nombre de failles a commencé à diminuer, mais les remontées étaient de plus en plus intéressantes, car les hunters « rentraient » dans notre produit et produisaient des rapports vraiment spécifiques à notre métier.

Après le premier mois, c'est devenu plus calme. Puis nous avons invité de nouveaux hunters afin d'avoir d'autres points de vue, d'autres compétences sur certains aspects spécifiques de notre programme.

Le programme privé a également permis à nos équipes de s'entraîner à traiter les rapports, à les classifier et les qualifier, et d'ajuster les règles.

Après cette phase de rodage, nous avons décidé de passer en programme public en avril 2018, soit 7 mois après l'ouverture de notre programme en privé.

Nous étions vraiment satisfaits de la qualité des échanges avec les hunters durant la phase privée, et n'étions donc pas inquiets sur le passage en public... Nous voulions simplement plus de hunters sur notre programme !

Il y avait aussi un message relativement fort qu'on voulait envoyer : n'importe qui trouvant une faille peut nous la remonter ! Bien entendu, nous avons reçu plus de rapports après le passage en programme public, mais c'était totalement gérable.

ANTONIN LE FAUCHEUX, CISO, BLABLACAR :

Aujourd'hui, nous nous efforçons d'obtenir des rapports de qualité, sur des failles toujours plus complexes, qui nécessitent plus de temps d'exploitation par les hunters, et des profils de hunters plus expérimentés.

Dans ce cadre, nous avons notamment augmenté le montant de nos primes pour les vulnérabilités critiques. L'enjeu est, avec l'aide de YesWeHack, d'attirer des chercheurs qui trouvent des choses intéressantes sans faire exploser notre budget de primes.

QUELLES SONT, SELON VOUS, LES VALEURS AJOUTÉES DU BUG BOUNTY FACE AUX SOLUTIONS TRADITIONNELLES COMME LE PENTEST ?

ANTONIN LE FAUCHEUX :

Pour moi, chaque outil a son utilité. L'avantage du Bug Bounty, c'est d'abord le crowdsourcing : quand on missionne un cabinet d'audit, on a quelques consultants à disposition, alors qu'avec le Bug Bounty, nous avons potentiellement des centaines ou des milliers de testeurs travaillant sur notre site.

Il y a ensuite la continuité, le 365/24/7, alors qu'un pentest se déroule généralement sur une durée limitée et apporte une photo à l'instant T. Cette continuité est essentielle pour détecter les bugs au plus tôt, alors que nous faisons des mises à jour très fréquentes sur nos applications.

Autre différentiant, le Bug Bounty induit une obligation de résultat, alors que le pentest n'implique qu'une obligation de moyens. Ce point est aussi intéressant pour notre communication interne, auprès de nos équipes : nous pouvons leur dire que nous rémunérons seulement des personnes qui trouvent des failles exploitables, plutôt que de les rémunérer « pour voir » s'ils trouveront quelque chose, sans cette obligation de résultat.

Le Bug Bounty est aussi un message fort adressé aux hackers. Beaucoup de sociétés ont longtemps menacé de poursuites les hackers qui leur remontaient des failles. Du coup, il y a comme un traumatisme chez certains hunters qui trouvent des failles et hésitent à contacter les sociétés concernées, par peur d'être mal reçus.

Avec notre Bug Bounty, nous lançons ce message très fort à la communauté : on souhaite que vous nous remontiez des failles et pour cela, on vous donne un cadre légal et sécurisé, avec un tiers de confiance entre nous pour que tout se passe correctement.

Ce message est très important pour nous car nous voulons que les hunters se disent « j'ai trouvé une vulnérabilité sur BlaBlaCar, je peux être récompensé pour ce travail de manière légale et sans prendre de risques ». Plutôt que certains finissent par aller vendre cette faille sur le marché noir...

COMMENT TRAITEZ-VOUS LES RAPPORTS EN INTERNE ?

ANTONIN LE FAUCHEUX :

Nous sommes plusieurs à gérer le programme de Bug Bounty et à recevoir les rapports de vulnérabilités. L'équipe sécurité est en charge de les traiter, fait une première qualification, afin de qualifier la gravité du bug, s'il nécessite une attention immédiate ou non. Si la faille s'avère complexe, nous en discutons en équipe.

Une fois la vulnérabilité qualifiée en interne, on notifie l'équipe concernée grâce à un système de ticketing proposé par la plateforme YesWeHack.

Ce système de ticketing nous permet de suivre l'avancée des équipes dans leur process de correction et de les relancer au besoin.

On passe ensuite à l'étape de vérification de la correction auprès du hunter. C'est souvent une formalité car on a généralement vérifié nous-mêmes, mais c'est toujours intéressant d'avoir un oeil extérieur, et parfois on a des surprises : le hunter nous indique que ce n'est pas correctement corrigé !

YES WE HACK

BlaBlaCar

AVEZ-VOUS PU OBSERVER DES CHANGEMENTS AU SEIN DE VOS ÉQUIPES DEPUIS QUE VOUS ÊTES EN BUG BOUNTY ?

ANTONIN LE FAUCHEUX :

L'aspect sécuritaire est aujourd'hui bien plus pris en compte. Dans nos formations internes, on ne parle plus de failles potentielles, mais on montre des cas concrets, des failles qui nous ont été remontées dans le cadre de notre programme, ce qui a beaucoup plus d'impact.

> **“ Le Bug Bounty s'intègre dans le workflow des équipes via le système de ticketing, l'idée étant que les failles de sécurité sont des tâches comme les autres.**

COMMENT LE BUG BOUNTY S'INTÈGRE DANS VOTRE DÉMARCHE AGILE ?

ANTONIN LE FAUCHEUX :

Le Bug Bounty s'intègre dans le workflow des équipes via le système de ticketing, l'idée étant que les failles de sécurité sont des tâches comme les autres, que l'on va déléguer aux équipes concernées avec le bon niveau de priorité.

Comme on livre en continu, la possibilité d'étendre nos périmètres sous programme en un clic nous permet de détecter des choses rapidement sur ces nouveaux périmètres ce qui nous rend plus agile : dès la mise à jour d'une application, nous pouvons la faire tester, prendre en compte les résultats, et mettre facilement en place une boucle de rétroaction.

LA PROCHAINE ÉTAPE DANS VOTRE STRATÉGIE DE BUG BOUNTY ?

ANTONIN LE FAUCHEUX :

La prochaine étape avec le Bug Bounty est de continuer à « fine-tuner » notre programme pour améliorer en permanence la qualité de nos rapports, attirer de meilleurs hunters, etc.

À PROPOS DE

YES WE HACK

Créé en 2013, YesWeHack est la première plateforme de Bug Bounty et de VDP en Europe.

Notre plateforme connecte plus de 23 000 experts en cybersécurité (« hackers éthiques ») répartis dans 170 pays avec des organisations de toutes tailles et de tous secteurs pour sécuriser leurs périmètres exposés et rechercher les vulnérabilités (bugs) de leurs sites web, applications mobiles, infrastructures et objets connectés.

YesWeHack gère des programmes privés (seulement accessibles sur invitation) et des programmes publics pour des milliers d'organisations à travers le monde, en conformité avec les réglementations européennes les plus strictes.

En plus de sa plateforme de Bug Bounty, YesWeHack offre également : un soutien à la création d'une politique de divulgation des vulnérabilités (VDP), une plateforme d'apprentissage pour les hackers éthiques appelée Dojo et une plateforme de formation pour les institutions éducatives, YesWeHackEDU.

⟶ CONTACTEZ-NOUS

⟶ CONSULTEZ NOTRE SITE

BlaBlaCar