ÉTUDE DE CAS

PROGRAMME PRIVÉ BUG BOUNTY

INSTITUTION FINANCIÈRE FRANÇAISE

Mars 2020

YES WE HACK

Qu'est-ce qui vous a décidé à lancer un programme de Bug Bounty ?

Expert Sécurité des Systèmes d'Information :

En toute honnêteté, je n'étais pas convaincu au début. J'avais rencontré plusieurs prestataires qui me disaient faire du Bug Bounty, mais j'avais surtout l'impression que c'était une activité de "tuilage" entre différentes missions de leurs pentesteurs, pas une activité construite et cadrée.

Puis j'ai rencontré YesWeHack, qui a su m'exposer des avantages qui répondaient à mes attentes en termes de sécurité. J'ai commencé à voir les choses différemment et j'ai franchi le pas début 2018. Nous avons lancé une première campagne de Bug Bounty sur un site que nous connaissions bien, et que l'on avait déjà fait tester de nombreuses fois ; choisir un périmètre "mature" me permettait de mieux maîtriser les coûts éventuels du programme.

Je m'attendais à ne recevoir pratiquement aucune remontée car nous en étions à notre 8ème test d'intrusion sur ce site depuis mon entrée en fonction, et le dernier test datait de la semaine précédente. On était donc plutôt confiant. **Mais le résultat nous a démenti : nous avons reçu de nombreux rapports de vulnérabilité, dont une critique une heure seulement après le lancement du programme.**

On sait aujourd'hui que cette vulnérabilité existait depuis un an et demi. Autrement dit, deux pentests étaient passés dessus sans la voir. Donc forcément, nous avons immédiatement été séduits par le Bug Bounty. (Rires)

Plus largement, quelles sont selon vous les valeurs ajoutées du Bug Bounty face au pentest ?

Je vois quatre valeurs ajoutées principales.

La première, celle qui m'a séduite au début, c'est le fait qu'on se rapproche vraiment de quelque chose de réel **: on ne va pas seulement chercher à avoir une vue exhaustive des vulnérabilités, mais on va taper tout de suite là où ça fait mal.** Cela se rapproche au plus près de ce que ferait une attaque réelle.

Le deuxième point qui est très important, étant donné la mouvance actuelle de l'agilité, c'est la continuité. Nous faisons des mises à jour très régulières de nos applications exposées sur internet (au moins une par mois) : cela devient donc très compliqué et très coûteux de faire du pentest à chaque mise en production. **Le Bug Bounty nous apporte une surveillance en continu.**

Le troisième point, c'est, de manière générale, l'efficacité et la qualité du travail des chercheurs. Sur des sites qu'on avait éprouvés de très nombreuses fois, on a systématiquement trouvé des vulnérabilités, dont certaines étaient critiques. Les chercheurs sont payés au résultat, donc, clairement, leur objectif est de trouver quelque chose de concret pour nous, et c'est aussi mon objectif. Un des problèmes du pentest, c'est que les résultats dépendent tellement du pentesteur…

Avec le Bug Bounty, on a vraiment des spécialistes à disposition. Les chercheurs ne vont pas forcément chercher toutes les typologies de vulnérabilités que l'on peut trouver sur une application web, ils vont là où ils sont forts, où ils sont efficaces rapidement. Et c'est ce que l'on recherche aussi. **Depuis que nous sommes en Bug Bounty, nous sommes passés un cran au-dessus en terme de sécurité** : on a trouvé des vulnérabilités inédites, on a pu les corriger, et la sécurité de ces applications est passée au niveau supérieur. **Finalement, c'est ça que l'on doit viser en tant que RSSI : pas seulement la conformité, mais plus de sécurité.**

Et enfin, dernier point mais pas des moindres : le ROI. Entre le budget primes et le coût de la plateforme, et aux vues des résultats, sur l'année, c'est très rentable. **J'ai plus de vulnérabilités significatives remontées pour un coût moindre qu'avec un pentest**, cela étant valable pour des applications matures et éprouvées de multiples fois.

Sur certains sites importants, je fais des pentests depuis des années et reçois des rapports vides ou quasi vides. **On le faisait parce que c'était notre politique et pour répondre à nos exigences de conformité, mais ça ne nous apportait plus rien ou presque en termes de sécurité.**

Le Bug Bounty c'est la mort du pentest ou c'est complémentaire ?

Cela reste complémentaire, mais ça va en réduire sérieusement le périmètre : on va essayer de garder le même nombre de pentests, mais en les focalisant sur des périmètres moins critiques.

Aujourd'hui, je me demande quel est l'intérêt de pentester annuellement des applications gérées en mode agile. Et pour toutes les applications critiques et exposées sur Internet, on va probablement transiter vers le Bug Bounty. En fait, c'est déjà en cours.

Comment fonctionne le Bug Bounty chez vous ? Avez-vous pu observer des changements sur vos équipes depuis que vous êtes en Bug Boutny ?

Nous sommes en "programme managé", c'est-à-dire que nous ne faisons pas nous-même le "triage " des vulnérabilités. Mais, en interne, je suis en charge du programme de Bug Bounty.
C'est un peu chronophage au début, il faut s'astreindre à une certaine discipline et ne pas tomber dans le piège qui serait d'aller regarder chaque vulnérabilité une par une, dès qu'on les reçoit. Une fois qu'on a trouvé son rythme (pour moi c'est une fois par semaine), c'est très efficace, et en termes de temps, on est proche de la gestion d'un projet de pentest classique. **En revanche, c'est beaucoup plus simple à lancer et à suivre qu'un pentest.**

On a donné à l'équipe de Sécurité Opérationnelle un accès direct à notre programme, ils peuvent ainsi voir les vulnérabilités à mesure qu'elles sont validées, et nos développeurs peuvent échanger directement avec les Chercheurs.

On les a impliqués dès le lancement du programme, ils ne l'ont pas du tout pris comme une "punition", mais plutôt comme un jeu d'attaque / défense, et c'est comme ça que je voulais que ça soit pris.
C'était : "Ah, ils sont forts, comment ils font ça ?" Etc. (Rires) **Cela nous a rendu beaucoup plus efficace. Ça les fait progresser et plus généralement, ça nous fait progresser en termes de sécurité.**

Comment le Bug Bounty s'intègre dans votre démarche agile ?

On avait déjà conscience qu'il fallait faire des choses, mais il nous était impossible de répondre au besoin de contrôle des applications en production en faisant des tests d'intrusions (mise en production tous les mois) – on en était à faire des mises en production sans vraiment respecter notre politique de sécurité, puisqu'on ne pouvait les auditer au fil de l'eau.

Il nous fallait donc trouver une autre solution, et cette solution, c'était le Bug Bounty. En fait, j'ai vraiment l'impression que le Bug Bounty EST conçu pour l'agilité.

On ne peut pas être agile en faisant du pentest, cela ne fonctionne pas : on ne peut pas suivre le rythme des projets, il y en a trop, et on ne peut pas en faire avant chaque mise en production, par manque de temps, de réactivité et de moyens : les délais sont trop courts, mouvants, et les tests doivent être planifiés plusieurs fois par an.

Le Bug Bounty nous a donc permis de lancer une vraie démarche de contrôle du DevOps, et de proposer une sécurité agile, en profondeur et en collaboration avec toutes les équipes concernées, sans trop les impacter, dans une logique d'amélioration continue.

Par exemple, lorsqu'une vulnérabilité est reçue, validée et transmise pour traitement, qu'on nous répond en interne que le Pare Feu Applicatif (WAF) a été mis à jour en conséquence, puis qu'on demande au Chercheur de vérifier et qu'il parvient toujours à exploiter la vulnérabilité en contournant le WAF d'une autre manière, ça nous permet de montrer qu'il est nécessaire de corriger le code, et on peut demander au Chercheur d'expliquer comment au développeur si besoin.

Chacun est à la fois responsabilisé, outillé, et beaucoup plus réactif, c'est aussi ça le DevSecOps.

YES WE HACK

A propos de YesWeHack : YesWeHack propose aux entreprises une approche disruptive de la cybersécurité : le Bug Bounty, modèle qui récompense les chercheurs à la vulnérabilité. Notre plateforme connecte plus de 15 000 experts en cybersécurité (« hackers éthiques ») répartis dans 140 pays et des organisations de toutes tailles et de tous secteurs pour rechercher les vulnérabilités (bugs) de leurs sites web, applications mobiles, infrastructures et objets connectés, et sécuriser leurs périmètres exposés. Avec sa plateforme (la #1 en Europe), YesWeHack apporte une solution efficace, agile et économique, faisant de la sécurité un moteur de la transformation digitale des entreprises.
www.yeswehack.com