ÉTUDE DE CAS

PROGRAMME PUBLIC BUG BOUNTY

INTERVIEW AVEC
ROMAIN LODS
HEAD OF ENGINEERING
DEEZER

Janvier 2020

YES WE HACK

deezer

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

Romain Lods, Head of Engineering, Deezer :

Environ deux ans avant de lancer notre programme de Bug Bounty, nous avons commencé à faire des audits de sécurité en interne sur notre code, ce qui n'avait jamais été fait avant chez Deezer.

Ces tests ont permis de faire une première passe et de corriger quelques grosses vulnérabilités.

Puis, par la force des choses, nous nous sommes intéressés au Bug Bounty et à YesWeHack.
La facilité d'usage de la plateforme a achevé de nous convaincre de l'intérêt de lancer un programme.

Quelles sont selon vous les valeurs ajoutées du Bug Bounty face aux solutions traditionnelles comme le pentest ?

Romain Lods, Head of Engineering, Deezer :

On réalise habituellement un audit par an, qui s'étend d'une à trois semaines sur plusieurs de nos services. Mais cette approche est coûteuse, se concentre à chaque fois sur quelques services seulement, et après des années, ne donne plus vraiment de résultats intéressants.

Le Bug Bounty nous permet d'avoir des remontées permanentes, tout au long de l'année, sur des périmètres variés, et de détecter des bugs rapidement après leur apparition.

En termes de ROI, le Bug Bounty est aussi très intéressant, on décide nous-même quelle prime on assigne à chaque vulnérabilité.

Le Bug Bounty nous garantit aussi une diversité de compétences des chercheurs. A contrario, un auditeur est ultra spécialisé, et on l'oriente un peu sur ce que l'on souhaite qu'il teste. **Avec le Bug Bounty, on a clairement été surpris de certains retours de chercheurs qui nous ont transmis les résultats de scénarios assez originaux, jamais vus auparavant.**

Enfin, j'apprécie la qualité des rapports sur les failles remontées via YesWeHack : on sent que les chercheurs essayent vraiment d'offrir un POC fonctionnel, reproductible, qu'on va pouvoir facilement retester chez nous.

Les rapports de nos audits habituels sont en général assez précis, mais **on retrouve également cette prévision dans le cadre du Bounty quand les chercheurs ont un bon niveau et jouent le jeu :** c'est alors très plaisant de recevoir leurs rapports illustrés de screenshots et de vidéos, ce qui facilite grandement leur compréhension, leur validation et leur communication aux équipes concernées.

Les échanges avec les chercheurs sont aussi facilités au travers de la plateforme quand il est nécessaire de préciser certains points.

Vous faites-vous aider par les chercheurs pour analyser et corriger les bugs reçus ?

Romain Lods, Head of Engineering, Deezer :

En effet, les chercheurs peuvent nous aider en phase de reproduction des bugs. De même, et dans certains cas, nous les sollicitons pour vérifier que la vulnérabilité a bien été corrigée.

Mais cela reste ponctuel dans la mesure où nous avons une grosse équipe de développeurs en interne qui prend en charge cette gestion des correctifs.

Pour vous, est-ce que le Bug Bounty c'est la mort du pentest, ou est-ce complémentaire ?

Romain Lods, Head of Engineering, Deezer :

Pour moi ça reste absolument complémentaire. Le Bug Bounty est un outil qui va plus loin que l'audit.

Comme je disais tout à l'heure, le pentest, tel qu'on le pratique jusqu'à maintenant, on le focalise sur des nouveaux services, ou sur des périmètres sur lesquels on sait déjà qu'il y a des problèmes.

Avez-vous pu observer des changements au sein de vos équipes depuis que vous êtes en Bug Bounty ?

Romain Lods, Head of Engineering, Deezer :

Il y a clairement une sensibilisation plus accrue à la sécurité. Nous avons déclenché de gros chantiers de sécurisation, suite à des retours de notre programme de Bug Bounty.

La vision a évolué et les choses ont changé par rapport à la cybersécurité, et le Bug Bounty est un des vecteurs de ce changement.

En termes de process, on collecte, trie et valide les rapports. Ensuite, sur la base des éléments de chaque rapport validé, un ticket interne est créé et assigné à l'équipe concernée pour traitement avec un degré de priorité déterminé.

Considèrez-vous le Bug Bounty comme un levier de confiance vis-à-vis du marché ?

Romain Lods, Head of Engineering, Deezer :

De mon point de vue, oui : **à travers un programme de Bug Bounty public, on démontre et on met en avant ses préoccupations de sécurité et de transparence.** On assume aussi le fait de s'exposer à des attaques, certes « maîtrisées », et de prendre en compte les retours critiques de la communauté.

Chez Deezer, nous avons une équipe dédiée à la lutte contre la fraude : en effet, les artistes et les labels sont rémunérés selon l'audience des pistes, et pour garantir leurs revenus, nous devons les prémunir de tout abus sur la plateforme. Ce sujet est donc crucial dans notre stratégie de sécurité – et dans le périmètre du Bug Bounty.

La prochaine étape ?

Romain Lods, Head of Engineering, Deezer :

Pour le moment, nous poursuivons notre stratégie actuelle, en relançant régulièrement l'activité du programme lorsque l'activité diminue.

D'une façon générale, le nombre de remontées dépend souvent de la visibilité dans l'actualité de Deezer, et quand nous faisons des opérations de communication, les chercheurs s'intéressent plus à notre programme.

Dans un second temps, nous envisagerons une augmentation des primes pour encourager les chercheurs à trouver des failles plus complexes.

Avez-vous un conseil pour des RSSI ou des start-tups qui se lancerait dans le Bug Bounty ?

Romain Lods, Head of Engineering, Deezer :

En règle générale, mieux vaut connaître ses failles de sécurité quand on débute dans un projet, que d'attendre qu'il y en ait trop à gérer, après qu'on ait fait de (mauvais) choix d'architectures.

Quand je vois ce que nous a remonté notre programme de Bug Bounty, je me dis que ça aurait été préférable que nous prenions en compte ces éléments le plus en amont possible. Donc, je conseillerais de ne pas attendre trop longtemps pour mettre en place des outils tels que le Bug Bounty, pour minimiser la dépendance aux systèmes hérités, plus complexes à sécuriser.

Romain Lods, Head of Engineering, Deezer