CYBERSÉCURITÉ
La finance a besoin de pirates

Les banques et les assurances font partie des entreprises les plus consommatrices de « bug bounty », des services de chasse de failles cyber…

PAR MORGANE REMY
+ EMAIL *redaction@agefi.fr*

***« Ne pas faire** appel aux hackers éthiques serait purement et simplement une erreur »*, annonce tout de go Mark Rampton, responsable de la cybersécurité chez Starling Bank. En effet, à son initiative, son employeur, la première banque 100 % digitale au Royaume-Uni, recourt à ce que l'on appelle le *bug bounty*, une mise à prix de vulnérabilités informatiques auprès de chasseurs de prime. La banque numérique ouvre un terrain de recherche à des pirates informatiques et les rémunère quand ils sont les premiers à détecter une faille. La récompense est à la hauteur du niveau de danger – de la criticité dit-on dans le secteur – de ladite faille. « *Pour résumer l'intérêt au recours au bug bounty pour notre banque, je réponds : excellent retour sur investissement* », poursuit Mark Rampton. En effet, en mettant à prix ses

ADOBE STOCK

propres failles informatiques, une entreprise a accès à des centaines de pirates éthiques et créatifs, avec des approches variées et le goût de la quête.

Cette banque numérique de l'autre côté de la Manche passe ainsi par Hacker One, une des plateformes de *bug bounty* les plus reconnues en Europe. Son rôle est de mettre en relation les entreprises, notamment de grandes banques et assurances françaises, et des *hackers* éthiques qu'ils ont sélectionnés. Selon le rapport 2021 Hacker-Powered Security Report de la plateforme, les primes versées par ce secteur s'élèvent à 2,45 millions de dollars, un chiffre très bas si on le compare au coût moyen d'une seule violation de données, estimé par IBM à 4,24 millions de dollars. Et la tendance s'accélère. « *Il y a eu une augmentation de 62 % de l'adoption de programmes faisant appels aux hackers éthiques par les organisations de services financiers en 2021* », détaille Chris Evans, responsable de la sécurité des systèmes d'information et *chief hacking officer* de cet intermédiaire, pour qui la finance représente 10 % de sa clientèle actuelle.

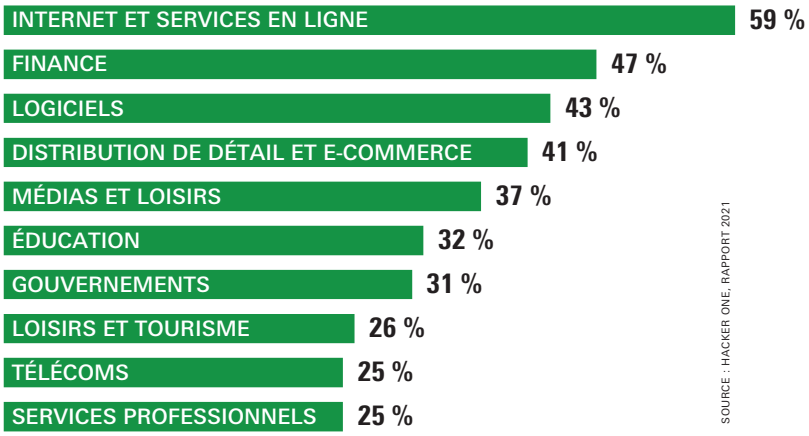
SÉLECTION

Cette pratique a souvent été adoptée en premier lieu par des start-up du numérique. Les *fintechs*, notamment les banques en ligne comme Starling Bank, doivent démontrer qu'elles sont à la fois à l'état de l'art en termes de cybersécurité et transparentes sur le sujet pour établir un lien de confiance avec leur clientèle. « *Pour nous, ce fut relativement simple de dupliquer notre offre bancaire sur le cloud destiné aux hackers, sans exposer nos services de production ou nos données sensibles*, rapporte Mark Rampton. « *Dans le secteur financier, les nouveaux acteurs ont clairement un avantage en matière de cybersécurité, grâce à leur architecture cloud-native.* » Mais ce n'est pas aussi évident pour les banques historiques qui doivent composer avec des couches logicielles qui s'imbriquent depuis plusieurs décennies.

Or c'est justement parce que les établissements bancaires ont développé un système informatique tentaculaire, parfois avec des applications non répertoriées (*shadow IT*) ou simplement qui ne peuvent plus être entretenues, notamment en langage Cobol où il y a une pénurie d'ingénieurs, que

AU DEUXIÈME RANG PARMI LES CLIENTS DES HACKERS

Part des secteurs parmi les utilisateurs



SOURCE : HACKER ONE, RAPPORT 2021

LE **BUG BOUNTY** CONSISTE EN UN OU PLUSIEURS PROGRAMMES DE SÉCURITÉ COLLABORATIVE, QUI S'APPUIENT SUR UNE COMMUNAUTÉ EXTERNE DE HACKERS ÉTHIQUES POUR DÉTECTER DES FAILLES DE SÉCURITÉ INCONNUES ET RÉDUIRE LE RISQUE CYBER. À TRAVERS CES PROGRAMMES, LES HACKERS REÇOIVENT DES PRIMES POUR LES FAILLES VALIDES IDENTIFIÉES.

cette recherche de failles peut avoir de la valeur. « *Dans ce secteur, j'ai trouvé de nombreuses vulnérabilités, par exemple une qui permettait d'utiliser des logiciels tiers et une autre qui me permettait de pénétrer dans les systèmes internes et, par exemple, de crypter toutes les données, comme le ferait un pirate malveillant*, raconte un *hacker* polonais connu sous le pseudonyme K4lin, qui définit sa motivation d'abord comme étant financière, ensuite relevant du challenge intellectuel. *Pour la deuxième faille, qui impliquait l'exécution de code à distance et pouvait conduire à un cryptage complet des données, j'ai reçu une prime de 15.000 dollars. Soit beaucoup moins que ce qu'aurait coûté une telle attaque malveillante, où obtenir le décryptage des données se monnaie en centaines de bitcoins.* »

Dans ce contexte, de plus en plus de banques traditionnelles et assureurs européens – comme BNP Paribas mais aussi SwissLife, Caixa Bank (en Espagne) et DZ Bank (en Allemagne) – se sont lancés. « *En France, les entreprises financières n'étaient clairement pas des précurseurs, mais elles représentent aujourd'hui le premier segment en volume*, témoigne Yassir Kazar, fondateur de la plateforme Yogosha, très reconnue dans l'Hexagone. *Il aura fallu un temps pour les rassurer sur notre capacité à sélectionner les hackers et cadrer le terrain d'action.* » Dans un premier temps, les banques et assurances s'inquiètent d'un double jeu de la part des *hackers* : revente de failles au plus offrant sur le *dark web*, utilisation de données personnelles pour organiser des fraudes ou intrusion dans le système permettant de demander une rançon. En bref, ces sociétés craignent de laisser entrer le loup dans la bergerie.

Les plateformes ont alors pour rôle de cadrer la partie, en sélectionnant les joueurs et le terrain de

Cadrer l'enveloppe budgétaire est impératif

jeu. « *Chez Yogosha, nous sommes une plateforme fermée où les hackers doivent passer des tests techniques mais aussi décliner leur identité, avec leur compte bancaire et leur numéro de Siret*, détaille Yassir Kazar. *Ensuite, imaginons le pire : un hacker veut revendre ce qu'il trouve sur le marché noir ; grand bien lui fasse car comme il s'agit d'un concours, il y aura toujours un deuxième pour trouver la même faille et réclamer la récompense.* » Eculée et corrigée, la brèche n'aura alors plus aucune valeur marchande… à condition que l'équipe interne de l'entreprise agisse vite. « *Le bug bounty est un merveilleux outil grâce à la compétition, encadré par des plateformes capables d'apporter des garanties sur le sérieux des hackers éthiques* », rebondit Brice Augras, *hacker* lui-même et désormais à la tête de sa propre entreprise de cybersécurité BZHunt basée à Brest.

Autre avantage : la récompense est proportionnelle au résultat. Mais cet atout est aussi à double tranchant car il faudra passer à la caisse à chaque trouvaille. Si l'enveloppe budgétaire est mal cadrée, le risque est de voir le client lésiner sur la criticité – c'est-à-dire le niveau de menace – pour faire baisser les primes à verser. « *J'ai eu du mal à collaborer avec des établissements bancaires qui minimisaient systématiquement la valeur de ce que nous trouvions*, confirme Roni Carta, 19 ans, développeur depuis ses 13 ans et, inspiré par Arsène Lupin, *hacker* professionnel et éthique depuis ses 16 ans. *Je m'en méfie désormais.* » « *Même une vulnérabilité à faible impact a tout de même une valeur significative, car elle donne une indication sur où se trouvent les faiblesses du système d'information*, répond Chris Evans, de Hacker One. *Nous encourageons les clients à récompenser les hackers éthiques généreusement.* »

TRAVAIL PRÉPARATOIRE

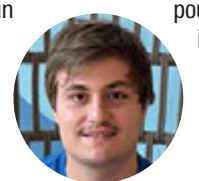
L'enjeu est de taille. « *Si un hacker se fait inviter sur une plateforme, puis dans des programmes privés exigeants, sur la base de sa réputation construite sur plusieurs années, l'inverse est vrai aussi*, rappelle Christophe Hautefeuille, *hacker* éthique réputé de la place travaillant sur les plateformes HackerOne mais aussi la troisième incontournable sur le Vieux Continent, Yes We Hack. *Quand un client est connu – et c'est le cas pour certaines entreprises en finance – pour remettre en cause en permanence la criticité de la faille et donc sa valeur, nous allons concentrer nos efforts ailleurs et il n'aura que des hackers inexpérimentés sur son programme.* » Pour être efficace et conserver une bonne réputation, il faut bien dimensionner l'enveloppe destinée au programme. « *Les failles jugées relativement critiques sont valorisées traditionnellement de 2.000 à 5.000 euros*, raconte Roni Carta. *Cela peut atteindre 200.000 à 500.000 euros dans la cryptomonnaie.* »

Pour ne pas se laisser déborder, les entreprises devront, avant d'ouvrir la chasse – un « programme » – trouver le maximum de problèmes par elles-mêmes. « *C'est ce qu'elles font toutes, avec plus ou moins de moyens et de maturité*, relate Brice Augras. *Elles réalisent alors en amont des tests d'intrusion où des équipes sont mobilisées pendant un nombre de jours donné pour tester le système d'information.* » Cela coûte entre 800 et 1.500 euros par jour en fonction des sociétés ; celles étant basées à Paris étant systématiquement au-dessus des 1.000 euros. Cette bonne pratique permet d'écluser ce qui est le plus évident et de n'avoir à payer des primes que pour ce qui est passé en dessous des radars classiques. ■

LA PAROLE À… **BENOIT MENARDO,** cofondateur de la fintech Payflow

« *Le bug bounty nous permet de renforcer la confiance des investisseurs* »

Quelles sont vos préoccupations en cybersécurité ?
Notre start-up, permettant à un salarié de recevoir au moment où il le souhaite une partie de son salaire, a deux ans d'existence. Dès les premiers mois, nous avons réussi à travailler pour de grandes entreprises. Dès 2020, un de nos clients nous a demandé de gérer les paies de plus de 5.000 salariés. Les données étant sensibles, il nous a posé un ultimatum sur la question de la cybersécurité. Nous avons dès lors passé la certification ISO 27001, le nec plus ultra en matière de sécurité des informations. Dans ce cadre, nous avons voulu nous confronter à la réalité et nous exposer à la communauté de *hackers* éthiques de Yogosha*. Au départ, j'avais quelques craintes malgré notre forte appétence pour la technologie, mais les contacts avec Yassir Kazar, fondateur de la plateforme, et son équipe ont permis de lever les derniers freins.



Comment collaborez-vous avec les hackers ?
Nous avons mis sur la table 5.000 euros pour éprouver notre système pendant une semaine et motiver des *hackers* capables de créativité. Résultat, très rapidement, quelques failles – toutes mineures, à ce stade – nous sont remontées. Nous avons ensuite mobilisé notre équipe trois à quatre semaines pour corriger tout ce qui avait été identifié. Nous envisageons de continuer de recourir à ce genre de programme régulièrement afin de rester toujours à l'état de l'art. Ainsi, quand nous développons notre solution, nous avons la garantie que nous construisons sur des fondations solides. C'est clairement un outil d'amélioration continue. Et cela est très utile pour gagner de nouveaux clients – les grands groupes nous demandant toujours plus de garanties en matière de cybersécurité – et pour renforcer la confiance des investisseurs qui soutiennent ou s'intéressent à Payflow.

*Plateforme de cybersécurité reposant sur une communauté de hackers certifiés pour la détection et la gestion des vulnérabilités et failles de sécurité.