Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Centre national pour la cybersécurité NCSC

NCSC

Questions et réponses - Programme de primes aux bogues au sein de l'administration fédérale

Version: 23.12.2022

Table des matières

1 Qu'est-ce qu'un programme de primes aux bogues?

Les programmes de primes aux bogues visent à repérer, à consigner et à corriger les éventuelles vulnérabilités des systèmes et applications informatiques avec l'aide de pirates éthiques. Ceux-ci emploient leurs propres méthodes afin de repérer des vulnérabilités souvent indétectables à l'aide d'un test d'intrusion ou d'un examen de sécurité classique.

2 Pourquoi l'administration fédérale recourt-elle à des programmes de primes aux bogues?

Les programmes de primes aux bogues représentent un outil précieux permettant non seulement aux entreprises, mais aussi à l'administration fédérale de détecter les vulnérabilités de leurs systèmes informatiques de façon proactive. Il s'agit d'une méthode efficace et financièrement avantageuse qui renforce la confiance que le public accorde aux systèmes testés (*public trust*). Les primes aux bogues reposent sur le principe de production participative qui consiste à exploiter le savoir-faire de la communauté spécialisée dans les questions de sécurité.

L'administration fédérale doit montrer l'exemple aux entreprises privées et à la société. En institutionnalisant les approches recourant aux primes aux bogues, au piratage éthique et à la production participative, elle encourage la cyberrésilience des infrastructures suisses.

3 Quel est le rôle du NCSC dans le programme de primes aux bogues?

Le NCSC est responsable du programme de primes aux bogues au sein de l'administration fédérale. Il est chargé de fournir et de gérer une plateforme centralisée destinée à réaliser les chasses aux bogues, de coordonner les programmes et de soutenir les unités administratives. En outre, il rend régulièrement compte des résultats des programmes de primes aux bogues au sein de l'administration fédérale.

Concrètement, le NCSC se charge de:

- planifier, prioriser et mettre en œuvre les programmes de primes aux bogues;
- soutenir les unités administratives dans la conception des programmes et gérer la plateforme destinée à la formation;
- assurer la coordination et la communication entre les unités administratives et Bug Bounty Switzerland SA (l'exploitant de la plateforme);
- gérer, sur le plan technique et administratif, la plateforme centralisée pour les programmes de primes aux bogues;
- réaliser, en collaboration avec Bug Bounty Switzerland, une évaluation technique et un tri des vulnérabilités;
- assurer la communication avec l'aide des unités administratives;
- garantir la conformité des processus de facturation et de paiement des programmes.

4 Pourquoi l'administration fédérale travaille-t-elle avec Bug Bounty Switzerland SA?

En août 2022, le NCSC a fait l'acquisition d'une plateforme centralisée pour les programmes de primes aux bogues afin de réaliser, en collaboration avec l'entreprise Bug Bounty Switzerland SA, des chasses aux bogues au sein de l'administration fédérale. Grâce à la plateforme dont s'est dotée la Confédération et à la grande communauté de pirates éthiques de Bug Bounty Switzerland SA, l'administration fédérale a tous les outils en main pour lancer de nouveaux programmes. Pionnière dans son domaine en Suisse, l'entreprise jouit d'une grande expertise en matière de chasse aux bogues et de collaboration avec des pirates éthiques.

5 Qu'est-ce qu'un «pirate éthique»?

Un pirate éthique ou un pirate bienveillant est un expert en cybersécurité mandaté pour vérifier des systèmes et des produits informatiques. Son objectif est de trouver les vulnérabilités qu'un pirate mal intentionné pourrait exploiter. Lors de cette opération, le pirate éthique respecte un cadre prédéfini, établi dans le programme de primes aux bogues, et signale les failles de sécurité découvertes sans en tirer parti. Une prime (*bounty*) plus ou moins élevée sera attribuée pour chaque faille détectée selon la gravité de celle-ci.

6 Quels sont les systèmes informatiques soumis aux programmes?

Ce sont les unités administratives de l'administration fédérale qui déterminent, en concertation avec le NCSC, quels systèmes sont soumis au test (*scope*).

7 Quel est le montant des primes (*bounties*)? Les montants sont-ils globalement prédéfinis?

Le montant de la prime varie en fonction de la gravité et de l'importance de la vulnérabilité détectée. Les primes sont déterminées par les unités administratives qui réalisent un programme de primes aux bogues, en collaboration avec le NCSC. Elles peuvent donc varier d'un programme à l'autre. Par souci de transparence, les primes potentielles sont déterminées au début d'un programme à l'aide d'une «grille de primes» et communiquées aux pirates éthiques.

8 Si des failles de sécurité sont découvertes, faut-il en déduire que la Confédération a mal travaillé et utilisé un système peu sûr? Pourquoi les failles signalées n'ont pas été décelées au préalable?

La technologie évolue rapidement et de nouvelles formes d'attaque se développent constamment, faisant de la sécurité informatique un processus évolutif. Les programmes de primes aux bogues visent à repérer, à consigner et à corriger les éventuelles vulnérabilités des systèmes et applications informatiques avec l'aide de pirates éthiques. Ceux-ci emploient leurs propres méthodes afin d'identifier des vulnérabilités souvent indétectables à l'aide d'un test d'intrusion ou d'un examen de sécurité classique.

9 N'est-il pas irresponsable de laisser des pirates informatiques accéder à des systèmes aussi importants?

Les pirates mandatés sont des pirates éthiques. Ils sont hautement qualifiés et adoptent un comportement particulièrement responsable lors de leur recherche de vulnérabilités. Par leur travail, ils souhaitent exercer une influence positive et contribuer au renforcement de la sécurité des systèmes testés. Pour participer, tous les pirates éthiques doivent en outre accepter les directives du programme et s'engager à respecter les règles énumérées.

10 Pourquoi les signalements de vulnérabilités ne sont-ils pas publiés dans leur intégralité?

Pour des raisons de sécurité, aucun détail concernant les vulnérabilités n'est dévoilé. Le NCSC publie toutefois une synthèse des résultats obtenus.

11 Les failles de sécurité détectées sont-elles toutes immédiatement corrigées? Que se passe-t-il lorsqu'un bogue est découvert?

Chaque vulnérabilité détectée fait immédiatement l'objet d'une analyse afin de déterminer les risques encourus. La procédure d'élimination des failles dépend donc du risque que la vulnérabilité soit exploitée et des dommages potentiels qui en découleraient. Cette évaluation permet de prioriser les vulnérabilités à corriger.

12 Selon quels critères les pirates sont-ils sélectionnés?

La sélection des pirates éthiques est effectuée par le NCSC, qui est responsable du programme de primes aux bogues de l'administration fédérale, en collaboration avec Bug Bounty Switzerland SA. Elle se fonde sur le périmètre du programme (*scope*) et les technologies concernées. L'expertise, les disponibilités du moment ainsi que les expériences positives acquises dans d'autres programmes similaires sont autant de critères décisifs lors de la sélection.

Chaque pirate éthique est soumis au préalable à une vérification de son identité et de son parcours (en anglais KYC - know your customer process) par Bug Bounty Switzerland SA.
Ainsi, l'entreprise garantit que seuls les pirates éthiques dont l'identité et l'intégrité ont pu être vérifiées pourront participer aux programmes et qu'aucune transaction ne sera effectuée avec des pirates éthiques figurant sur une liste de sanctions, par exemple.
Pour participer, tous les pirates éthiques doivent en outre accepter les directives du programme et s'engager à respecter les règles énumérées.
La plupart du temps, les systèmes à tester sont librement accessibles sur Internet. Ils ne nécessitent pas d’autorisation supplémentaire, étant donné qu'ils sont généralement à la disposition du grand public. La collaboration avec des pirates éthiques permet d'évaluer de manière réaliste les risques existants et de les restreindre le plus rapidement possible.

13 Les pirates éthiques qui participent aux programmes viennent-ils uniquement de Suisse?

Les pirates éthiques proviennent aussi bien de Suisse que de l'étranger. L'objectif est de tirer profit du large éventail d'expertises et de faire bon usage de l’intelligence collective.

14 D'autres programmes de primes aux bogues sont-ils prévus prochainement? Où puis-je trouver davantage d'informations à ce sujet?

Le programme de primes aux bogues au sein de l'administration fédérale teste et intègre continuellement de nouveaux systèmes. Le NCSC rend régulièrement compte de l'avancement des travaux. Pour de plus amples informations, veuillez consulter notre site Internet.

15 Le NCSC propose-t-il également son programme de primes aux bogues à l'administration publique des communes et cantons?

Pour l'instant, le programme de primes aux bogues du NCSC n'est proposé qu'aux unités administratives de l'administration fédérale. Nous examinons actuellement si ce service peut être proposé aux cantons et aux communes et, le cas échéant, dans quelle mesure.

16 Comment les programmes de primes aux bogues sont-ils financés?

La plateforme centralisée de primes aux bogues ainsi que la prestation de base pour la réalisation de tels programmes au sein de l'administration fédérale sont financées de manière centralisée par le NCSC. Les primes, quant à elles, sont toujours versées par le département ou l'unité administrative qui réalise le programme.

17 Combien de temps dure un programme de primes aux bogues?

La durée d'un programme est définie par le NCSC, en accord avec l'unité administrative chargée de sa réalisation. Ainsi, un programme peut durer quelques semaines, mais il peut également être conçu de telle sorte à ce que les recherches se fassent de façon continue et sans qu'une fin de programme nette soit définie.

18 Quelle est la différence entre un programme de primes aux bogues privé et public?

Dans le cadre d'un programme de primes aux bogues privé, les pirates éthiques ne peuvent participer que sur invitation (s'ils respectent les critères d'admission mentionnés plus haut). Cela signifie que le pilotage et l'ajustement du nombre de participants sont assurés par la gestion du programme.

Un programme de primes aux bogues semi-privé est rendu public, mais les détails du programme ne sont pas divulgués et les participants ne peuvent prendre part au programme

qu'après avoir réussi une procédure de recrutement (si les critères d'admission mentionnés plus haut sont respectés). Là aussi, le nombre de participants dépend de la gestion du programme.

Les programmes de primes aux bogues publics sont ouverts à tous les spécialistes intéressés, y compris au grand public. Les participants ne sont soumis à aucun critère d'admission spécifique.

19 Comment se déroule un programme de primes aux bogues?

La première étape consiste à définir les objectifs du programme de primes aux bogues ainsi qu'à établir les rôles et les procédures. Ensuite, un programme est élaboré sur la plateforme de primes aux bogues de Bug Bounty Switzerland SA, assorti de la définition de l'ensemble des conditions-cadres pertinentes (périmètre, grilles des primes, régime de protection, etc.).

Dans le cas d'un programme de primes aux bogues privé (voir question précédente), les pirates éthiques choisis reçoivent une invitation. Leur nombre peut être progressivement augmenté si nécessaire. Les failles détectées sont validées par Bug Bounty Switzerland SA et le NCSC, puis communiquées à l'unité administrative concernée pour qu'elle procède à leur correction.

Des réunions de mise au point plus ou moins régulières peuvent être organisées selon les besoins, mais il est également possible de ne réaliser qu'un débriefing à la fin du programme.

20 Les pirates éthiques sont-ils autorisés à continuer leurs recherches de vulnérabilités une fois le programme de primes aux bogues achevé?

Les directives du programme déterminent la période durant laquelle les pirates éthiques sont autorisés à rechercher des vulnérabilités et par conséquent recevoir des primes. En dehors de cette période, les vulnérabilités détectées peuvent être signalées à tout moment via le formulaire Coordinated Vulnerability Disclosure. Toutefois, aucune prime ne sera attribuée.

21 Les programmes se limitent-ils aux environnements de test ou sont-ils également appliqués aux systèmes de production?

En principe, les programmes de primes aux bogues sont réalisés au sein des systèmes de production et dans des conditions réalistes, afin de maximiser le bénéfice des connaissances. Toutefois, des tests peuvent exceptionnellement être effectués au sein des systèmes de test ou de systèmes similaires aux systèmes de production. La décision est prise en collaboration avec l'unité administrative concernée.

22 Dans quelle mesure les programmes de primes aux bogues peuvent-ils contribuer, sur le plan stratégique, à la sécurité des infrastructures des administrations et des entreprises?

Chaque système informatique contient très probablement des vulnérabilités encore inconnues. Un programme de primes aux bogues permet généralement de les détecter rapidement et en toute fiabilité. Collaborer avec des pirates éthiques est un moyen très efficace d'améliorer la sécurité de ses systèmes informatiques, tout en renforçant la confiance que le public accorde aux systèmes testés (*public trust*).

23 Où sont publiés les résultats des programmes de primes aux bogues?

Les résultats des programmes de primes aux bogues sont communiqués par les unités administratives en accord avec le NCSC. Ce dernier rend régulièrement compte des résultats des programmes de primes aux bogues sur son site Internet. Toutefois, aucun détail technique concernant les vulnérabilités n'est dévoilé.