

27 nov 2024 -14:00

L'administration fédérale belge invite les hackers éthiques à participer à la première édition de l'événement "Hack the Government"

Le Centre pour la Cybersécurité Belgique (CCB) organise *Hack the Government 2024*, le tout premier événement consacré au hacking éthique organisé par l'administration fédérale belge. Ce mercredi 27 novembre en soirée, le Premier ministre belge, Alexander De Croo, remettra au vainqueur de l'événement le prix très convoité de "Ethical Government Hacker of 2024".

*" Dans un esprit d'innovation et de sécurité, nous avons ouvert une sélection de ressources numériques de l'administration fédérale aux hackers éthiques. Nous reconnaissons la nécessité de mesures de sécurité robustes et nous croyons au pouvoir de l'intelligence collective. Cette entreprise n'était pas sans risque, mais nous avons pris avec confiance une mesure audacieuse pour renforcer les cyberdéfenses de la Belgique. Et les résultats sont à la hauteur et nous sommes fiers de l'engagement, du dévouement et de la détermination de ces hackers éthiques exceptionnels ". — Alexander De Croo, Premier ministre belge*

*Hack the Government 2024* est fermement ancré dans la conviction que les hackers éthiques peuvent accroître le niveau de cybersécurité en Belgique: un point de vue qui a amené la Belgique à autoriser le hacking éthique, moyennant le respect de certaines conditions strictes définies par la loi.

Cette initiative sans précédent rassemble la communauté des hackers éthiques dans le but d'identifier des failles de sécurité sur des sites web ou des systèmes publics. Nous pouvons faire de la Belgique le pays le moins cyber vulnérable de l'UE.

L'événement *Hack the Government 2024* accueille une équipe plurielle de hackers éthiques, alliant professionnels et étudiants, déterminés à consolider la cybersécurité des ressources numériques belges. Ils uniront leurs forces pour mettre les systèmes publics à l'épreuve. Bien que la compétition vise à décerner le titre de "*Ethical Government Hacker of 2024*", le travail d'équipe est stimulé par le biais du mentorat, de la collaboration et du partage entre les participants.

Les entités publiques fédérales participant à cette initiative sont les suivantes:

- Service public fédéral Stratégie et Appui (SPF BOSA)
- L'Office national des vacances annuelles (ONVA)
- L'Agence fédérale des médicaments et des produits de santé (AFMPS)
- Le Centre pour la Cybersécurité Belgique (CCB)

*Hack The Government 2024* est organisé en étroite collaboration avec la plateforme Intigrity pour les chasseurs de vulnérabilités (*bug bounty*), ce qui donne une occasion unique de mettre les systèmes publics à l'épreuve par le biais de tests de pénétration contrôlés et autorisés. Lancé le 13 novembre, le défi se terminera par un événement en présentiel le mercredi 27 novembre. Le/la lauréat·e de *Hack The Government 2024* gagnera une formation dispensée par le célèbre SANS Institute, y compris l'examen de certification par la Global Information Assurance Certification (GIAC), d'une valeur de plus de

10 000 euros. Sans oublier la touche d'humour informatique: nous avons également prévu des mentions honorables pour divers prix humoristiques, notamment "Le/la premier(-ère) à frapper un grand coup" et "Le/la champion(ne) des duplicatas".

L'importance du hacking éthique et des programmes de récompenses (*Bug Bounty*)

Les exercices tels que les tests de pénétration (*pentests*) et les programmes de primes aux chasseurs de bugs permettent aux organisations de s'attaquer de manière proactive aux risques liés à la cybersécurité. Ces organisations peuvent ainsi garder une longueur d'avance sur les cybermenaces et renforcer la confiance du public dans les services numériques.

*"Il s'agit d'un moment historique pour la Belgique. En invitant des hackers éthiques à tester ses défenses numériques, l'administration fédérale fait preuve d'un véritable leadership en matière de cybersécurité. Ces efforts de collaboration avec la communauté des hackers éthiques fournissent une couche de protection inestimable, et je suis ravi de voir que l'administration fédérale montre l'exemple aux autres".*  
— Inti De Ceukelaire, hacker en chef d'Intigriti

L'événement se terminera par une cérémonie de remise des prix présidée par le directeur général du CCB, Miguel De Bruycker, qui a souligné la valeur de cette collaboration:

*"Hack The Government 2024 met à l'honneur les dispositions légales (ci-dessous) en vigueur depuis le 15 février 2023 qui autorisent le hacking éthique en Belgique. Cela ne veut pas dire que c'est facile! Les hackers éthiques doivent respecter des conditions strictes. Le CCB travaille avec des hackers éthiques sélectionnés pour montrer ce qui peut être fait tout en améliorant nos défenses et en construisant une culture de résilience en matière de cybersécurité au sein de l'administration. C'est très stimulant pour nous car nous exposons également nos propres sites web. Ces pirates ambitieux découvrent en ce moment même les vulnérabilités de nos infrastructures. Nous y voyons une occasion de renforcer notre cyber protection".*

Ce travail ne s'achèvera d'ailleurs pas le 27 novembre. La vérification des résultats, la validation des processus et procédures, et les ajustements nécessaires pour améliorer la cybersécurité se feront en continu pour être testés à nouveau à l'avenir.

*"L'AFMPS se réjouit de participer à Hack the Government 2024. Alors que nous recherchons continuellement l'excellence pour assurer la sécurité de la santé publique, nous considérons la cybersécurité comme un élément crucial de notre mission, en particulier en ce qui concerne la conformité à la loi NIS2. Nous croyons au pouvoir du hacking éthique en tant qu'outil pour renforcer notre infrastructure numérique. Nous sommes convaincus que la collaboration et les enseignements que nous tirerons de cette initiative renforceront encore nos systèmes et nos services".* — Pierre Colangelo, Infrastructure ICT (AFMPS)

*"L'ONVA est extrêmement fier de faire partie de Hack The Government 2024. En tant qu'organisation au service des citoyens, nous reconnaissons l'importance de mesures de cybersécurité solides pour protéger leurs données. Cette initiative visant à inviter des hackers éthiques à tester nos systèmes informatiques est donc le moyen idéal de renforcer de manière proactive notre sécurité numérique." - Myriam DEMOL, Déléguée à la protection des données - Déléguée à la sécurité de l'information (ONVA)*

Cette initiative représente une avancée majeure dans le domaine de la cybersécurité au niveau fédéral, en

réunissant des entités publiques, des experts privés et la communauté du hacking éthique. *Hack The Government 2024* souligne l'importance de la collaboration en matière de cybersécurité. Nous sommes enthousiastes à l'idée de dévoiler les fruits de cette initiative pionnière.

### Politique nationale en matière de signalement des vulnérabilités

L'événement sera organisé dans le cadre des dispositions de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS2) . Il s'agit du cadre juridique belge qui permet aux personnes de signaler au Centre pour la Cybersécurité Belgique (CCB) et à l'organisation concernée des vulnérabilités identifiées dans des systèmes d'information sans craindre de poursuites pénales ou civiles, à condition de respecter certaines règles. Ce cadre juridique permet de renforcer les défenses numériques de la Belgique en encourageant la participation du public aux efforts de cybersécurité et d'encadrer adéquatement de telles actions.

Ce type d'événement encourage également les organisations en Belgique, comme les administrations publiques fédérales, à développer une politique de divulgation coordonnée des vulnérabilités (CVDP) leur permettant de recevoir le signalement de vulnérabilités (avec des canaux de communication appropriés).

Chaque organisation peut éventuellement aussi offrir un programme de Bug Bounty (offrant des récompenses financières pour les vulnérabilités détectées), incitant ainsi les experts à contribuer à la sécurité des services publics.

Centre pour la Cybersécurité Belgique  
Rue de la Loi 18  
1000 Bruxelles  
Belgique  
<http://www.ccb.belgium.be>

Michele Rignanese  
Porte-parole(NL/FR/E)  
+32 (0)477 38 87 50  
[michele.rignanese@ccb.belgium.be](mailto:michele.rignanese@ccb.belgium.be)

Katrien Eggers  
Porte-parole(NL/FR/E)  
+32 485 76 53 36  
[katrien.eggerts@ccb.belgium.be](mailto:katrien.eggerts@ccb.belgium.be)