25 nov 2026 -10:01

Hack the Government 2026 : un record de participation pour la troisième édition

Le Centre pour la Cybersécurité Belgique (CCB) organise aujourd'hui l'événement de clôture de Hack the Government (HTG) 2026 . Cette initiative invite des hackers éthiques sélectionnés à tester des systèmes d'institutions publiques belges dans des conditions légalement contrôlées. L'objectif est de détecter et de signaler les vulnérabilités avant que des acteurs malveillants ne les trouvent.

Une édition record. Cette année, en une semaine seulement, nous avons reçu près de deux fois plus de soumissions de vulnérabilités que l'année dernière sur l'ensemble des deux semaines. Cette hausse s'explique, outre le rôle de soutien joué par l'IA, par la participation de quatre organismes publics supplémentaires.

77 participants, 12 systèmes. HTG 2026 réunit 45 hackers éthiques professionnels et 32 étudiants. Ils testent 12 systèmes gouvernementaux, contre 4 en 2024 et 8 en 2025. Parmi les organisations participantes figurent le SPF Justice, la Police fédérale, l'AFMPS, Belnet et la Défense. Cette croissance témoigne d'une relation de plus en plus mature entre les institutions publiques et la communauté des hackers éthiques

Pourquoi c'est essentiel. L'incident PHP2Shell d'octobre 2026 a rappelé ce qui se passe quand la divulgation coordonnée échoue. L'embargo a été levé de fait avant le déploiement des correctifs, ce qui a provoqué des maintenances d'urgence dans des banques, des services publics et chez des hébergeurs. Parallèlement, l'IA accélère le développement d'exploits. Détecter et corriger les failles de façon proactive, grâce à des chercheurs de confiance, est donc plus important que jamais.

Un cadre juridique de pointe. La loi NIS2 du 26 avril 2024 protège les hackers éthiques qui divulguent des vulnérabilités de bonne foi. Le CCB assure la coordination nationale et la médiation avec les organisations concernées.

"Hack the Government illustre ce que nous défendons au CCB : la sécurité se renforce par la collaboration. Cette année, le CCB a de nouveau mis ses propres systèmes à l'épreuve, aux côtés des autres institutions. Le nombre de signalements reçus témoigne de l'engagement de la communauté des hackers éthiques et de la maturité croissante des institutions publiques. Mieux vaut qu'une faille soit découverte par un chercheur de confiance que par un acteur malveillant."

Miguel De Bruycker
Directeur général du Centre pour la Cybersécurité Belgique (CCB)

Et après ? Les vulnérabilités validées sont communiquées aux seules organisations concernées et au CCB, qui suit leur correction. Les résultats finaux seront publiés à l'issue de l'événement.

"À l'heure où nos services en ligne prennent une place toujours plus importante, il est crucial de continuer à mettre nos applications à l'épreuve. C'est pourquoi le SPF Justice a participé cette année pour la première fois à Hack The Government. Cette initiative précieuse nous permet de porter un regard externe et critique sur notre sécurité et de déceler d'éventuelles vulnérabilités. Nous pouvons ainsi renforcer proactivement nos systèmes face aux futures cybermenaces. De plus, cet événement constitue pour nous une excellente opportunité de nous profiler comme un service public moderne et accessible, et d'attirer de nouveaux talents IT."

Marc Duforez
Conseiller général – directeur ICT, SPF Justice

Infos presse – Quartier Papier, Fabrieksstraat 55/59, 1930 Zaventem.

Interviews de 12h30 à 13h30, avec Miguel De Brucyker, directeur général du CCB. La presse est la bienvenue jusqu'à la remise des prix.

Dossier de presse

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

Katrien Eggers
Porte-parole(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

© 2026 - news.belgium.be