25 Nov. 2026 -10:01

Hack the Government 2026: Rekordbeteiligung bei der dritten Ausgabe

Das Zentrum für Cybersicherheit Belgien (ZCB) veranstaltet heute die Abschlussveranstaltung von Hack the Government (HTG) 2026 . Die Initiative lädt ausgewählte ethische Hacker ein, Systeme belgischer öffentlicher Einrichtungen unter rechtlich abgesicherten Bedingungen zu testen. Ziel ist es, Schwachstellen zu erkennen und zu melden, bevor böswillige Akteure sie finden.

Eine Rekordausgabe. In diesem Jahr gingen innerhalb nur einer Woche fast doppelt so viele Schwachstellenmeldungen ein wie im Vorjahr im gesamten Zeitraum von zwei Wochen. Dieser Anstieg lässt sich neben der unterstützenden Rolle der KI auch durch die Teilnahme von vier zusätzlichen öffentlichen Einrichtungen erklären.

77 Teilnehmer, 12 Systeme. HTG 2026 vereint 45 professionelle ethische Hacker und 32 Studierende. Sie testen 12 Regierungssysteme, verglichen mit 4 im Jahr 2024 und 8 im Jahr 2025. Zu den teilnehmenden Organisationen zählen der FÖD Justiz, die Föderale Polizei, die FAGG, Belnet und die Landesverteidigung. Dieses Wachstum zeugt von einer zunehmend reifen Beziehung zwischen den öffentlichen Einrichtungen und der Community der ethischen Hacker.

Warum das entscheidend ist. Der Vorfall PHP2Shell im Oktober 2026 hat vor Augen geführt, was geschieht, wenn die koordinierte Offenlegung scheitert: Die Sperrfrist wurde faktisch aufgehoben, bevor die Patches bereitstanden, was Notfallwartungen bei Banken, öffentlichen Diensten und Hosting-Anbietern auslöste. Zugleich beschleunigt KI die Entwicklung von Exploits. Schwachstellen mithilfe vertrauenswürdiger Forscher proaktiv zu erkennen und zu beheben, ist daher wichtiger denn je.

Ein solider rechtlicher Rahmen. Das NIS2-Gesetz vom 26. April 2024 schützt ethische Hacker, die Schwachstellen in gutem Glauben melden. Das ZCB übernimmt die nationale Koordination und die Vermittlung zwischen den Forschern und den betroffenen Organisationen.

> "Hack the Government zeigt, wofür wir beim ZCB stehen: Sicherheit wird durch Zusammenarbeit gestärkt. In diesem Jahr hat das ZCB neben den anderen Einrichtungen erneut seine eigenen Systeme auf die Probe gestellt. Die Zahl der eingegangenen Meldungen zeugt vom Engagement der Community der ethischen Hacker und von der wachsenden Reife der öffentlichen Einrichtungen. Es ist besser, wenn eine Schwachstelle von einem vertrauenswürdigen Forscher entdeckt wird als von einem böswilligen Akteur."

Miguel De Bruycker
Generaldirektor, Zentrum für Cybersicherheit Belgien

Wie geht es weiter? Die validierten Schwachstellen werden ausschließlich den betroffenen Organisationen und dem ZCB mitgeteilt, das deren Behebung nachverfolgt. Die Endergebnisse werden nach Abschluss der Veranstaltung veröffentlicht.

"In einer Zeit, in der unsere Onlinedienste immer mehr an Bedeutung gewinnen, ist es entscheidend, unsere Anwendungen kontinuierlich auf die Probe zu stellen. Deshalb hat der FÖD Justiz in diesem Jahr erstmals an Hack the Government teilgenommen. Diese wertvolle Initiative ermöglicht uns einen externen, kritischen Blick auf unsere Sicherheit und deckt mögliche Schwachstellen auf. So können wir unsere Systeme proaktiv gegen künftige Cyberbedrohungen stärken. Darüber hinaus bietet uns die Veranstaltung eine hervorragende Gelegenheit, uns als moderner und zugänglicher öffentlicher Dienst zu positionieren und neue IT-Talente zu gewinnen."

Marc Duforez
Generaldirektor – ICT-Leiter, FÖD Justiz

Presseinformationen – Quartier Papier, Fabrieksstraat 55/59, 1930 Zaventem.

Interviews mit Miguel De Bruycker, Generaldirektor des ZCB, finden von 12:30 bis 13:30 Uhr statt. Die Presse ist bis zur Preisverleihung herzlich willkommen.

Dossier de presse

Zentrum für Cybersecurity Belgien
Rue de la Loi 18
1000 Brüssel
Belgien
http://www.ccb.belgium.be

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

Michele Rignanese
Sprecher(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

© 2026 - news.belgium.be