27 Nov. 2024 -14:00

Belgische Bundesregierung lädt ethische Hacker zum ersten 'Hack the Government'-Event ein

Das Zentrum für Cybersicherheit Belgien (CCB) veranstaltet "*Hack the Government 2024*", die erste von der belgischen Regierung organisierte Veranstaltung für ethisches Hacken. Am Mittwochabend, dem 27. November, wird Alexander De Croo, der belgische Premierminister, dem Gewinner der Veranstaltung die begehrte Auszeichnung "Ethical Government Hacker of 2024" überreichen.

"Im Geiste der Innovation und Sicherheit haben wir ausgewählte digitale Ressourcen der Bundesregierung für ethische Hacker geöffnet. Wir sind uns der Notwendigkeit robuster Sicherheitsmaßnahmen bewusst und glauben an die Macht der kollektiven Intelligenz. Dieses Unterfangen war nicht ohne Risiko, aber wir haben einen mutigen Schritt zur Stärkung der belgischen Cyberabwehr unternommen. Die Ergebnisse sind da, und wir sind stolz auf das Engagement, die Hingabe und die Entschlossenheit dieser außergewöhnlichen ethischen Hacker.
- *Alexander De Croo, Premierminister von Belgien*

Die Vorbereitungen für das Finale von Hack the Government 2024 am Mittwoch sind fest in der Überzeugung verwurzelt, dass ethische Hacker jedem in Belgien helfen können, das Internet sicherer zu machen. Diese Ansicht hat dazu geführt, dass das Gesetz anerkennt, dass ethisches Hacken in Belgien legal sein kann.

Diese beispiellose Initiative bringt die Gemeinschaft der ethischen Hacker zusammen, um Schwachstellen in den Websites und Systemen der Regierung aufzuspüren und so Belgiens Engagement für Cybersicherheit und proaktive Verteidigungsmaßnahmen zu demonstrieren. Gemeinsam können wir Belgien zum am wenigsten gefährdeten Land in der EU machen

Hack the Government 2024 wird von einer Gruppe ethischer Hacker (Fachleute und Studenten) organisiert, die dazu beitragen wollen, die digitalen Ressourcen Belgiens sicherer zu machen. Sie werden sich zusammentun, um die Regierungssysteme auf den Prüfstand zu stellen. Diese Zusammenarbeit bietet den Teilnehmern die seltene Gelegenheit, direkt zur Sicherung der öffentlichen Infrastruktur beizutragen. Obwohl es sich um einen Wettbewerb handelt, bei dem es darum geht, "Ethical Government Hacker of 2024" zu werden, entwickelt sich die Teamarbeit durch Mentoring, Zusammenarbeit und Austausch unter den Teilnehmern.

Die an dieser Initiative beteiligten staatlichen Stellen sind:

- FPS Politik und Unterstützung (FOD BOSA/SPF BOSA)
- L'Office national des vacances annuelles / Rijksdienst voor jaarlijkse vakantie (ONVA/RJV)
- Föderale Agentur für Arzneimittel und Gesundheitsprodukte (FAMHP/FAMPS/FAGG)
- Das Zentrum für Cybersicherheit Belgien (CCB)

Hack The Government 2024 wird in enger Zusammenarbeit mit der renommierten Bug-Bounty-Plattform

Intigriti organisiert und bietet eine einzigartige Gelegenheit, Regierungssysteme durch kontrollierte, autorisierte Penetrationstests auf die Probe zu stellen. Der Wettbewerb begann am 13. November und findet seinen Höhepunkt in einer persönlichen Veranstaltung am Mittwoch, den 27. November. Derjenige, der zum "Ethical Government Hacker of 2024" gekürt wird, gewinnt einen Schulungskurs des renommierten SANS Institute, einschließlich der Prüfung zur Global Information Assurance Certification (GIAC) im Wert von über 10 000 Euro. Eine Prise IT-Humor darf natürlich nicht fehlen, und so haben wir unter auch Reihe von lustigen Preisen ausgelobt, darunter "Der erste, der Blut vergießt" und "Derjenige, der die meisten Duplikate einreicht".

Die Bedeutung von Ethical Hacking und Bug Bounty-Programmen

Durch Übungen wie Penetrationstests (Pentests) und Bug Bounty-Programme gehen Organisationen proaktiv gegen Cybersicherheitsrisiken vor, sind Cyberbedrohungen immer einen Schritt voraus und stärken das Vertrauen der Öffentlichkeit in digitale Dienste.

"Dies ist ein bahnbrechender Moment für Belgien. Indem sie ethische Hacker einlädt, ihre digitale Verteidigung zu testen, zeigt die Bundesregierung eine echte Führungsrolle im Bereich der Cybersicherheit. Diese Zusammenarbeit mit der Ethical-Hacking-Community bietet einen unschätzbaren Schutz, und ich bin begeistert, dass die Bundesregierung ein Beispiel für andere setzt." - *Inti De Ceukelaire, Chief Hacker Officer von Intigriti*

Den Abschluss der Veranstaltung bildet eine Preisverleihung unter der Leitung des Generaldirektors des CCB, *Miguel De Bruycker*, der den Wert dieser Zusammenarbeit hervorhob:

Hack The Government 2024“ hebt die seit dem 15. Februar 2023 geltenden gesetzlichen Bestimmungen (siehe unten) hervor, die ethisches Hacking in Belgien erlauben. Das heißt aber nicht, dass es einfach ist! Ethische Hacker müssen strenge Bedingungen erfüllen. Das CCB arbeitet mit ausgewählten ethischen Hackern zusammen, um zu zeigen, was möglich ist, und gleichzeitig unsere Verteidigung zu verbessern, was zu einer Kultur der Widerstandsfähigkeit im Bereich der Cybersicherheit innerhalb der Regierung führt. Für uns ist das ziemlich aufregend, weil wir auch unsere eigenen CCB-Websites offenlegen. Diese ehrgeizigen Hacker entdecken gerade jetzt Schwachstellen in unseren Infrastrukturen. Wir sehen dies als eine Gelegenheit, unseren Cyberschutz zu stärken."

Hack the Government bedeutete, dass die Bundesbehörden der CCB vertrauten, den Prozess zu leiten und zu organisieren. Dies bedeutete eine enge Zusammenarbeit über mehrere Monate, um den Umfang der Veranstaltung im Detail festzulegen. Die Arbeit wird jedoch nicht am 27. November enden. Die Überprüfung der Ergebnisse, die Validierung von Prozessen und Verfahren und die Vornahme notwendiger Anpassungen zur Verbesserung der Cybersicherheit werden fortgesetzt, um auch in Zukunft getestet zu werden.

"Das FAGG freut sich, Teil von Hack the Government 2024 zu sein. Da wir ständig nach Spitzenleistungen bei der Gewährleistung der öffentlichen Gesundheitssicherheit streben, sehen wir die Cybersicherheit als einen entscheidenden Teil unserer Aufgabe, insbesondere in Bezug auf die Einhaltung des NIS2-Gesetzes. Wir glauben an die Macht des Ethical Hacking als Instrument zur Stärkung unserer digitalen Infrastruktur. Wir sind zuversichtlich, dass die Zusammenarbeit und die Lehren, die wir aus dieser Initiative ziehen, unsere Systeme und Dienste weiter stärken werden." - *Pierre Colangelo*, IKT-Infrastruktur (FAGG)

"Das RJV ist sehr stolz darauf, Teil von Hack The Government 2024 zu sein. Als eine Organisation im

Dienste der Bürgerinnen und Bürger wissen wir, wie wichtig starke Cybersicherheitsmaßnahmen zum Schutz ihrer Daten sind. Diese Initiative, die ethische Hacker einlädt, unsere IT-Systeme zu testen, ist daher der ideale Weg, um unsere digitale Sicherheit proaktiv zu stärken." - *Myriam DEMOL, Data protection officer (RJV)*

Diese Initiative stellt einen großen Fortschritt in der Cybersicherheit von Behörden dar, da sie öffentliche Einrichtungen, privates Fachwissen und die Ethical-Hacking-Community zusammenbringt. *Hack The Government 2024* unterstreicht die Bedeutung der Zusammenarbeit im Bereich der Cybersicherheit, und wir freuen uns darauf, die Ergebnisse dieser Pionierarbeit zu präsentieren.

Nationale Politik zur Meldung von Schwachstellen.

Die Veranstaltung wird im Rahmen der Bestimmungen des Gesetzes vom 26. April 2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netzen und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (NIS-Gesetz2) organisiert. Dabei handelt es sich um den belgischen Rechtsrahmen, der es Personen ermöglicht, dem Zentrum für Cybersicherheit Belgien (CCB) und der betreffenden Organisation identifizierte Schwachstellen in Informationssystemen zu melden, ohne eine straf- oder zivilrechtliche Verfolgung befürchten zu müssen, sofern sie bestimmte Regeln einhalten. Dieser Rechtsrahmen ermöglicht es, die digitale Verteidigung Belgiens zu stärken, indem er die Beteiligung der Öffentlichkeit an den Bemühungen um Cybersicherheit fördert und einen angemessenen Rahmen für solche Aktionen schafft.

Diese Art von Veranstaltung ermutigt auch Organisationen in Belgien, wie die föderalen öffentlichen Verwaltungen, eine Politik der koordinierten Offenlegung von Schwachstellen (CVDP) zu entwickeln, die es ihnen ermöglicht, die Meldung von Schwachstellen (mit geeigneten Kommunikationskanälen) entgegenzunehmen.

Jede Organisation kann eventuell auch ein Bug-Bounty-Programm anbieten (mit finanziellen Belohnungen für entdeckte Schwachstellen) und so Experten dazu bringen, zur Sicherheit der öffentlichen Dienste beizutragen.

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