27 nov 2024 -14:00

Belgische Federale Overheid nodigt ethische hackers uit voor allereerste 'Hack the Governement'-evenement

Het Centrum voor Cybersecurity België (CCB) organiseert *Hack the Government 2024*, het allereerste ethische hackingevenement georganiseerd door de Belgische federale overheid. Op woensdagavond 27 november zal eerste minister, Alexander De Croo de felbegeerde "Ethische Overheidshacker van 2024"-prijs uitreiken aan de winnaar van het evenement.

"In de geest van innovatie en veiligheid hebben we een aantal digitale systemen van de federale overheid opengesteld voor ethische hackers. We erkennen de noodzaak van robuuste beveiligingsmaatregelen en we geloven in de kracht van collectieve intelligentie. Dit initiatief was niet zonder risico, maar we hebben een gedurfde stap gezet om de cyberdefensie van België te versterken. De resultaten zijn er en we zijn trots op de inzet, toewijding en vastberadenheid van deze uitzonderlijke ethische hackers." - Alexander De Croo, Eerste Minister van België

Hack de Government 2024 wil aantonen dat ethische hackers kunnen helpen om België cyberveiliger te maken. In België is ethisch hacken in de wet verankerd en kunnen ethische hackers binnen een welomschreven kader te werk gaan.

Dit nooit eerder geziene initiatief brengt de gemeenschap van ethische hackers samen om kwetsbaarheden in overheidswebsites en -systemen te identificeren. Samen kunnen we van België het minst cyberkwetsbare land in de EU maken.

Om het nog spannender te maken, is *Hack the Government 2024* samengesteld uit een gevarieerde groep ethische hackers (professionals en studenten) die meehelpen om de Belgische digitale omgeving veiliger te maken. Deze samenwerking geeft deelnemers een unieke kans om rechtstreeks bij te dragen aan het beveiligen van de overheidsinfrastructuur. Hoewel het een wedstrijd is om "Ethische Overheidshacker van 2024" te worden, moedigen we ook samenwerking aan tussen de meer en minder ervaren deelnemers.

De overheidsdiensten die deelnemen aan dit initiatief zijn:

- FOD Beleid en Ondersteuning (FOD BOSA/SPF BOSA)
- Rijksdienst voor jaarlijkse vakantie (ONVA/RJV)
- Het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG)
- Het Centrum voor Cybersecurity België (CCB)

Hack The Government 2024 wordt georganiseerd in nauwe samenwerking met het bug bounty platform Intigriti en biedt een unieke kans om overheidssystemen op de proef te stellen door middel van gecontroleerde, geautoriseerde penetratietests. De uitdaging begon op 13 november en wordt afgerond tijdens een evenement op woensdag 27 november. Degene die wordt gekroond tot "Ethical Government Hacker of 2024" wint een training van het SANS Institute, inclusief het Global Information Assurance Certification-examen (GIAC) ter waarde van meer dan € 10.000. Een vleugje IT-humor mag niet ontbreken, dus we hebben ook eervolle vermeldingen voorzien voor verschillende ludieke prijzen, waaronder "The first to draw blood" and "The one submitting most duplicates".
Het belang van ethisch hacken en bug bounty-programma's

Door middel van penetratietests (pentests) en bug bounty-programma's pakken organisaties proactief cyberbeveiligingsrisico's aan, blijven ze cyberbedreigingen voor en versterken ze het vertrouwen van het publiek in digitale diensten.

"Dit is een mijlpaal voor België. Door ethische hackers uit te nodigen om haar digitale verdediging te testen, toont de federale overheid echt leiderschap in cyberbeveiliging. Deze samenwerking met de ethische hackersgemeenschap biedt een onschatbare laag bescherming. De federale overheid is een voorbeeld voor anderen." - *Inti De Ceukelaire, Chief Hacker Officer van Intigriti*

Het evenement wordt afgesloten met een prijsuitreiking onder leiding van *Miguel De Bruycker*, directeur-generaal van het CCB, die de waarde van deze samenwerking benadrukte:

"Hack De Overheid 2024" belicht de wettelijke bepalingen (zie hieronder) die sinds 15 februari 2023 van kracht zijn en die ethisch hacken in België toestaan. Dit betekent niet dat alles zomaar toegestaan is. Ethische hackers moeten zich aan strikte voorwaarden houden. Het CCB werkt samen met geselecteerde ethische hackers om te laten zien wat er mogelijk is en tegelijkertijd onze verdediging te verbeteren. Het is heel spannend voor ons omdat we ook onze eigen CCB-websites laten hacken. Deze ambitieuze hackers ontdekken op dit moment kwetsbaarheden in onze infrastructuren. We zien dit als een kans om onze cyberbescherming te versterken."

Het werk eindigt niet op 27 november. Het controleren van de bevindingen, het valideren van processen en procedures en het maken van de nodige aanpassingen om de cyberbeveiliging te verbeteren, zullen in de toekomst opnieuw worden getest.

"FAGG is verheugd om deel uit te maken van Hack the Government 2024. Omdat we voortdurend streven naar uitmuntendheid in het waarborgen van de veiligheid van de volksgezondheid, zien we cyberbeveiliging als een cruciaal onderdeel van onze missie, vooral met betrekking tot de naleving van de NIS2-wet. We geloven in de kracht van ethisch hacken als middel om onze digitale infrastructuur te versterken. We zijn ervan overtuigd dat de samenwerking en de lessen die we uit dit initiatief trekken, onze systemen en diensten verder zullen versterken." - *Pierre Colangelo*, ICT Infrastructuur (FAGG)

"De RJV is bijzonder trots om deel uit te maken van Hack The Government 2024. Als een organisatie die ten dienste staat van de burgers erkennen we het belang van sterke cybersecuritymaatregelen om hun gegevens te beschermen. Dit initiatief om ethische hackers uit te nodigen onze IT-systemen te testen is dan ook de ideale manier om onze digitale beveiliging proactief te versterken." - *Myriam DEMOL, Data protection officer-Information security officer*

Dit initiatief betekent een grote stap voorwaarts op het gebied van cyberbeveiliging bij de overheid en brengt overheidsinstanties, particuliere expertise en de gemeenschap van ethische hackers samen. *Hack The Government 2024* benadrukt het belang van samenwerking op het gebied van cyberbeveiliging en we kijken uit naar de resultaten van deze baanbrekende inspanning.

Nationaal beleid voor het melden van kwetsbaarheden

Het evenement wordt georganiseerd onder de bepalingen van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van algemeen belang voor

de openbare veiligheid (NIS2). Dit is het Belgische wettelijke kader dat personen in staat stelt om vastgestelde kwetsbaarheden in informatiesystemen te melden aan het Centrum voor Cybersecurity België (CCB) en de betrokken organisatie zonder vrees voor strafrechtelijke of burgerrechtelijke vervolging, op voorwaarde dat bepaalde regels worden nageleefd. Dit wettelijke kader maakt het mogelijk om de digitale verdediging van België te versterken door de deelname van het publiek aan inspanningen op het gebied van cyberbeveiliging aan te moedigen en een passend kader te bieden voor dergelijke acties.

Dit type evenement moedigt organisaties in België, zoals de federale overheidsadministraties, ook aan om een gecoördineerd beleid voor de bekendmaking van kwetsbaarheden (CVDP) te ontwikkelen, zodat ze meldingen van kwetsbaarheden kunnen ontvangen (via de juiste communicatiekanalen).

Elke organisatie zou ook een Bug Bounty-programma kunnen aanbieden (met financiële beloningen voor ontdekte kwetsbaarheden) en zo experts aanmoedigen om bij te dragen aan de beveiliging van overheidsdiensten.

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
België
http://www.ccb.belgium.be

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

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