HACK THE GOVERNMENT

2026 — SLOTEVENEMENT

PERSMAP

Woensdag 25 november 2026 | Centrum voor Cybersecurity België (CCB)

1. Praktische informatie voor de pers

Evenement: Hack the Government 2026 | Slotevenement

Datum: woensdag 25 november 2026

Locatie: Quartier Papier | Fabrieksstraat 55/59, 1930 Zaventem

Persinformatie: katrien.eggers@ccb.belgium.be

De pers is van harte welkom om het volledige dagprogramma **bij te wonen** tussen 9:00 en 17:00. – Gelieve aanwezigheid te bevestigen per mail katrien.eggers@ccb.belgium.be, of bericht 0485 76 53 36

Tijdvenster voor interviews: 12.00 – 13.00 uur

De volgende vertegenwoordigers staan tussen 12.00 en 13.00 uur ter beschikking van de pers:

Miguel De Bruycker — Directeur-generaal, Centrum voor Cybersecurity België (CCB)

2. Waarom gecoördineerde bekendmaking van kwetsbaarheden (CVD) belangrijk is

Cyberkwetsbaarheden horen bij het digitale leven. De vraag is niet óf ze bestaan, maar hoe snel en hoe verantwoord ermee wordt omgegaan zodra ze worden ontdekt. Gecoördineerde bekendmaking van kwetsbaarheden (CVD) is het gestructureerde proces waarbij onderzoekers kwetsbaarheden melden aan de getroffen organisatie en aan een betrouwbare autoriteit, zodat ontwikkelaars de tijd krijgen om het probleem op te lossen **voordat** er misbruik van kan worden gemaakt.

België beschikt over een van de meest vooruitstrevende CVD-kaders van Europa. De **Belgische NIS2 wet van 2024** biedt expliciete bescherming aan ethische hackers die te goeder trouw kwetsbaarheden ontdekken en verantwoord melden, ook wanneer er geen formeel bugbountyprogramma bestaat. Het CCB fungeert als nationaal coördinatiepunt: het ontvangt de meldingen en bemiddelt tussen de onderzoeker en de organisatie bij het verhelpen van de kwetsbaarheid (meer informatie in **bijlage 1** en op de webpagina van het CCB over CVD).

Recente casus: het PHP2Shell-incident (oktober 2026)

Hoe belangrijk een robuust CVD-proces is, bleek in oktober 2026 duidelijk uit de PHP2Shell-kwetsbaarheid: een kritieke kwetsbaarheid in PHP, een van de meest gebruikte server-side talen op het web, waarmee code op afstand kan worden uitgevoerd. Op 21 oktober 2026 verschenen gepatchte versies, maar de gecoördineerde bekendmaking **liep mis** nog voordat de oplossing op grote schaal was toegepast. Uitgelekte CVE-identificaties, een per ongeluk vrijgegeven video en het vroegtijdig verspreiden van patches door sommige leveranciers schonden het embargo. Dat veroorzaakte een golf van spoedonderhoud bij banken, overheidsdiensten, gamingplatformen en webhostingproviders.

> **De les:** wanneer het gecoördineerde bekendmakingsproces werkt, krijgen verdedigers een voorsprong. Loopt het mis (door een lek, een voortijdige publicatie of een nagelaten melding), dan zijn aanvallers aan de slag nog voordat de patch beschikbaar is. PHP2Shell is een schoolvoorbeeld van waarom het CVD-proces rigoureus, betrouwbaar en wettelijk verankerd moet zijn.

Het PHP2Shell-incident illustreert ook een bredere trend: niet-gepatchte of net onthulde kwetsbaarheden in veelgebruikte technologieën komen snel in het vizier van aanvallers. Hack the Government levert een directe bijdrage aan het nationale CVD-ecosysteem. Het leidt de volgende generatie onderzoekers op in verantwoorde bekendmaking en test overheidssystemen onder wettelijk gecontroleerde omstandigheden door, voordat kwaadwillenden dezelfde zwakke plekken kunnen ontdekken.

---

3. AI en de kwetsbaarheidsrace: wat de feiten laten zien

Artificiële intelligentie verandert de snelheid waarmee aanvallers exploits ontwikkelen en inzetten. De aanwijzingen zijn inmiddels sterk genoeg om te stellen dat **AI de ontwikkeling van exploits en de automatisering van aanvallen versnelt**.

Wat onafhankelijke gegevens laten zien

AI verkort de tijd waarin kwetsbaarheden worden misbruikt, maar er bestaat **geen universele „tijd tot exploitatie”**. De publicatie van exploitcode, de eerste waargenomen exploitatie door een aanvaller en de officiële opname in een Known Exploited Vulnerabilities (KEV)-catalogus zijn drie afzonderlijke mijlpalen, elk met een eigen tijdlijn.

Recente gegevens tonen aan dat bepaalde waardevolle kwetsbaarheden, vooral in internetgerichte en edge-technologieën, **al binnen enkele uren na bekendmaking, of zelfs daarvoor**, kunnen worden misbruikt. AI-systemen kunnen inmiddels belangrijke fasen van kwetsbaarheidsonderzoek en exploitontwikkeling automatiseren, en aanbieders van dreigingsinformatie signaleren die mogelijkheden stilaan in concrete aanvallen.

Toch **wordt de meerderheid van de bekendgemaakte kwetsbaarheden in de praktijk nooit actief misbruikt**. Het beschikbare onderzoek laat bovendien niet toe te zeggen in hoeverre AI de tijd tussen bekendmaking en daadwerkelijk misbruik heeft ingekort voor alle Common Vulnerabilities and Exposures (CVE’s).

Waarom dit HTG nog belangrijker maakt

Als AI de tijd tussen bekendmaking en misbruik van waardevolle doelwitten verkort, wordt het pleidooi voor **proactief, ethisch speurwerk door betrouwbare menselijke onderzoekers alleen maar sterker**. Kwetsbaarheden opsporen en verhelpen voordat ze publiek bekend raken, is een race geworden waarin verdedigers er niet langer van uit kunnen gaan dat ze weken of maanden de tijd

hebben. Hack the Government zet de juiste mensen, met de juiste wettelijke bescherming, aan de juiste kant van die race.

4. De rol van het CCB: een community uitbouwen

Als nationale autoriteit op vlak van cybersecurity speelt het Centrum voor Cybersecurity België een dubbele rol in Hack the Government: het is zowel **organisator** als **actieve partner** en helpt overheidsdiensten om, vaak voor het eerst, constructief samen te werken met de community van ethische hackers.

HTG 2026 omvat 12 overheidssystemen, bijna het drievoud van de eerste editie in 2024. Verschillende organisaties, waaronder de FOD Justitie, de Federale Politie, het FAGG-AFMPS en Defensie, nemen dit jaar deel. Die groei weerspiegelt een steeds hechtere relatie tussen overheidsdiensten en de ethische hackers, gesteund door het vooruitstrevende Belgische wettelijke kader voor CVD (**zie bijlage 1**).

Drie edities: de resultaten in één oogopslag

Meting	Editie 1 — 2024	Editie 2 — 2025	Editie 3 — 2026
Deelnemers	—	71	77
waarvan senioren / professionals	—	39	45
waarvan studenten	—	32	32
Ingediende kwetsbaarheidsrapporten	154	352	Wordt live bekendgemaakt Maar dit jaar werden in 1 week al meer kwetsbaarheden gevonden dan vorig jaar gedurende de 2 weken
Gevalideerde kwetsbaarheden	85	98	Wordt live bekendgemaakt
waarvan kritiek / uitzonderlijk	7	20	—
waarvan hoog	15	12	—
Deelnemende overheidsdiensten	4	8	12

De volledige factsheet kunt u opvragen

5. Getuigenissen van deelnemers

Hack the Government is meer dan een wedstrijd. Voor veel deelnemers is het een keerpunt in hun loopbaan: een eerste echte kennismaking met professionele offensieve beveiliging, een kans om een

netwerk op te bouwen en het bewijs van vaardigheden die geen enkel certificaat volledig kan vervangen. Drie getuigenissen uit eerdere edities:

> **„Hack the Government was veel meer dan een hackwedstrijd. Het was een belangrijke stap in mijn loopbaan."**
>
> **Pedro (alias: drop)** | Freelance consultant offensieve beveiliging; Senior Penetration Tester voor een langdurige opdracht in de overheidssector; co-captain van het Belgische HackerOne-nationaal team
>
> *Pedro nam deel aan de eerste editie van HTG (2024) en eindigde op de derde plaats. Hij maakte de overstap vanuit marketing en datawetenschap en gebruikte bugbountyprogramma's en HTG om zijn vaardigheden in de praktijk te bewijzen. Dat leverde hem uiteindelijk een langlopende opdracht bij een grote internationale instelling, plus een uitnodiging om België te vertegenwoordigen op de HackerOne World Cup.*

> **„Dat we in België binnen de richtlijnen in feite alles mogen hacken en daar nog erkenning voor krijgen, is geweldig en wereldwijd uniek."**
>
> **Logan** | Masterstudent in het laatste jaar; actief bugbountyjager; bijdrager aan het nationale CVD-programma van het CCB
>
> *Hij droeg al twee jaar vóór het einde van zijn studie bij aan CVD en gebruikte HTG om een netwerk op te bouwen. Dat leidde rechtstreeks tot kwetsbaarheden die hij alleen nooit had gevonden.*

> **„Evenementen zoals HTG tonen aan dat hackers en overheid kunnen samenwerken in plaats van tegenover elkaar te staan, en zo bouw je betere beveiliging op."**
>
> **Timothy** | Bugbountyjager; richtte in juni 2026 zijn eigen cyberbeveiligingsbedrijf op; nam op 16-jarige leeftijd voor het eerst deel aan HTG
>
> *Timothy's eerste HTG was een koude douche: hij vond vrijwel niets. Hij kwam terug en eindigde in 2025 als zevende. Zijn beslissing om een eigen bedrijf op te richten schrijft hij toe aan de mentaliteit die hij via HTG ontwikkelde.*

De volledige getuigenissen kunt u opvragen.

6. Veelgestelde vragen

Wat is een ethische hacker?

Oorspronkelijk verwees de term 'hacker' naar mensen met een passie voor sleutelen: experts die systemen doorgronden en tot het uiterste testen. In de cyberbeveiliging is een **ethische hacker** een kwetsbaarheidsjager die legaal en constructief te werk gaat: hij spoort beveiligingsfouten op en meldt ze verantwoord, in plaats van ze voor eigen gewin uit te buiten. Het zijn in feite verdedigers die denken als aanvallers.

Wat is Hack the Government?

Hack the Government (HTG) is een initiatief van het CCB waarbij gescreende ethische hackers worden uitgenodigd om de IT-systemen van Belgische overheidsinstellingen te testen onder wettelijk gecontroleerde omstandigheden. Het enige doel is kwetsbaarheden verantwoord op te sporen en te melden voordat kwaadwillenden ze kunnen vinden. Het is een oprechte uitnodiging tot samenwerking tussen de hackergemeenschap, de overheid en de academische wereld.

Zijn deelnemers wettelijk beschermd?

Ja. Op grond van de Belgische wet van 26 april 2024 en het nationale CVD-kader van het CCB zijn deelnemers wettelijk beschermd als ze te goeder trouw handelen: ze beperken zich tot wat strikt noodzakelijk is, hebben geen kwaadwillige bedoelingen en melden hun bevindingen aan de verantwoordelijke organisatie en aan het CCB.

Wie kan deelnemen?

HTG 2026 brengt **77 deelnemers** samen: 45 ervaren ethische hackers en professionals en 32 studenten. Deelnemers worden geselecteerd via een aanmeldingsprocedure en moeten strikte deelnamevoorwaarden aanvaarden. Het programma combineert bewust verschillende ervaringsniveaus en wil de talentkloof dichten door studenten in een live, praktijkgerichte omgeving in contact te brengen met ervaren professionals.

Welke systemen worden getest?

Tijdens HTG 2026 worden 12 overheidssystemen getest, waaronder systemen van de FOD Justitie en de Federale Politie. De organisaties nemen vrijwillig deel en de scope van elk systeem wordt vooraf vastgelegd. Bevindingen worden uitsluitend gedeeld met de verantwoordelijke organisaties en het CCB en worden tijdens het evenement niet openbaar gemaakt.

Wat gebeurt er na het evenement?

Alle gevalideerde kwetsbaarheden worden gedeeld met de betrokken organisaties, die instaan voor het verhelpen ervan. Het CCB volgt de opvolging via zijn proces voor gecoördineerde bekendmaking. De definitieve resultaten van HTG 2026 worden na het evenement gepubliceerd.

Contact: Persdienst CCB
Michele Rignanese |michele.rignanese@ccb.belgium.be | +32 477 38 87 50
Katrien Eggers |katrien.eggers@ccb.belgium.be | +32 485 76 53 36

Alle redactionele en statistische informatie is correct per 19 november 2026 en kan worden herzien in afwachting van de definitieve resultaten van HTG 2026.

CVD IN BELGIË

Kwestbaarheid gevonden?

CENTRE FOR CYBERSECURITY BELGIUM

Meld het. Help het verhelpen.

Bij gecoördineerde bekendmaking van kwetsbaarheden (CVD) meldt u een lek vertrouwelijk, zodat de verantwoordelijken het kunnen verhelpen.

HET BEKENDMAKINGSPROCES [1, 3]

1. **Lees de regels**
   Bekijk het CVD-beleid van de organisatie, als dat er is. Respecteer het toepassingsgebied en volg de meldinstructies.
2. **Controleer voorzichtig**
   Doe alleen wat nodig is om het lek te bevestigen. Vermijd verstoringen en onnodige toegang tot gegevens.
3. **Meld het vertrouwelijk**
   Meld aan de organisatie wat getroffen is en hoe het probleem te reproduceren is. Gebruik een beveiligd kanaal.
4. **Werk mee aan een oplossing**
   De organisatie onderzoekt het lek en werkt aan een oplossing. Blijf in contact; het CCB kan helpen coördineren.
5. **Stem eventuele publicatie af**
   Publicatie is niet verplicht. Bij de wettelijke procedure moet u vóór publicatie toestemming van het CCB krijgen.**

OPTIONELE WETTELIJKE PROCEDURE [2]

Bescherming naar Belgisch recht

Met of zonder CVD-beleid van de organisatie.

Meld zo snel mogelijk, uiterlijk binnen:

24 uur

Eerste rapport

Identificeer het systeem en beschrijf het lek kort.

72 uur

Volledig rapport

Geef de reproductiestappen en de belangrijkste technische details.

BEIDE RAPPORTEN GAAN NAAR

Organisatie + CCB

Beide termijnen starten bij de ontdekking.*

RESPECTEER DE VOORWAARDEN [1, 2]

Handel te goeder trouw
Geen bedreiging, afpersing of misbruik van gegevens.

Controleer vóór u test
Sommige gevoelige organisaties eisen vooraf schriftelijk akkoord.

Ken de grenzen
Bescherming is voorwaardelijk en geldt alleen onder Belgisch recht.

Gebruik de CCB-formulieren en instructies voor veilig indienen [2]

vulnerabilityreport@ccb.belgium.be

* Ontdekking: het moment waarop u redelijkerwijs een mogelijke kwetsbaarheid zou moeten herkennen, na redelijk onderzoek en validatie.

** De termijn van 90 dagen begint bij een formeel publicatieverzoek aan het CCB.
Als vóór het verstrijken van die termijn geen weigering is meegedeeld, kan de publicatie als toegestaan worden beschouwd.

CCB = Centrum voor Cybersecurity België

Samenvatting in heldere taal | 19 november 2026

[1] ccb.belgium.be/regulation/cvdp
[2] ccb.belgium.be/cert/vulnerability-reporting-ccb
[3] CCB-gids, deel I: proces

AI en de jacht op kwetsbaarheden:

Wat de gegevens werkelijk onthullen

Persbijlage | Hack the Government 2026 | Centrum voor Cyberveiligheid België 25 november 2026

1. De exploitatietermijn[1] is geen op zichzelf staande indicator

In berichtgeving over door AI versnelde cyberdreigingen wordt de 'exploitatietijd' vaak voorgesteld als één enkel, vergelijkbaar cijfer. Dat klopt niet. In openbare rapporten lopen minstens vier verschillende tijdsreferenties door elkaar, waardoor de cijfers niet rechtstreeks vergelijkbaar zijn.

Indicator	Wat het werkelijk meet	Waarom dit belangrijk is	Essentiële waarschuwing
Bekendmaking van de CVE[2] → openbare exploit / PoC[3]	Tijdsduur tot de publicatie van een exploitcode of een proof-of-concept	Meet de openbare beschikbaarheid van een exploit, niet het gebruik ervan door aanvallers	Beschikbaarheid van de exploit ≠ gebruik in de praktijk
Bekendmaking van de CVE → eerste waargenomen misbruik	Tijd die verstrijkt voordat er geloofwaardig bewijs opduikt dat aanvallers de kwetsbaarheid in de praktijk misbruiken	Meet de exploitatie in de praktijk	De waarneming kan plaatsvinden na de eerste daadwerkelijke aanval
Exploitatie vóór de bekendmaking	De exploitatie vindt plaats vóór de openbare bekendmaking van de CVE of de beschikbaarheid van een patch	Klassiek zero-daygeval: het tijdsverschil kan negatief zijn	De openbaarmaking van de CVE is niet het startpunt van de race
Publicatie van de CVE → opname in de KEV-lijst[4]	Tijd die een leverancier van dreigingsinformatie nodig heeft om voldoende bewijs te verzamelen om een CVE als 'uitgebuit' te classificeren	Weerspiegelt zowel de tijd die nodig is voor bevestiging en melding als de activiteit van de aanvallers	De opname in de KEV vindt plaats na de daadwerkelijke exploitatie

Het Amerikaanse agentschap voor cyberveiligheid (CISA) maakt een expliciet onderscheid tussen een **openbaar proof-of-concept (PoC) en actieve exploitatie**. Om een exploitatie als 'actief' te kwalificeren, is gedeeld, waarneembaar en betrouwbaar bewijs nodig dat kwaadwillende actoren de kwetsbaarheid in reële omstandigheden hebben gebruikt. VulnCheck baseert zijn analyse op dezelfde manier op het *eerste*

[1] In de Engelstalige literatuur aangeduid als *„time-to-exploit"* of TTE.
[2] **CVE** (*Common Vulnerabilities and Exposures*, oftewel 'veelvoorkomende kwetsbaarheden en blootstellingen') is een openbare catalogus en een systeem van unieke identificatiecodes waarin bekende IT-beveiligingslekken worden geregistreerd.
[3] In de cyberbeveiliging is een proof of concept (vaak **PoC** genoemd, afkorting van *proof of concept*) een concrete demonstratie die het bestaan van een IT-lek of kwetsbaarheid aantoont, meestal met behulp van een programma of een testmethode.
[4] Op het gebied van cyberbeveiliging is de **KEV-lijst** (of *de 'Known Exploited Vulnerabilities'-catalogus*, in het Nederlands vertaald als 'bekende uitgebuite kwetsbaarheden') een openbaar register dat wordt bijgehouden door CISA, het Amerikaanse agentschap voor cyberbeveiliging.

bewijs van exploitatie en niet louter op de datum waarop de exploitcode verscheen. Dit onderscheid verklaart de schijnbare tegenstrijdigheden tussen de cijfers van verschillende leveranciers.

2. Wat onafhankelijke gegevens aan het licht brengen

VulnCheck — Analyse van misbruikgevallen in de eerste helft van 2026

VulnCheck onderzocht 495 kwetsbaarheden waarvan het misbruik in de eerste helft van 2026 voor het eerst werd vastgesteld:

- **23,43 %** vertoonde tekenen van misbruik **op of vóór de publicatiedatum van de CVE** (aanvallers waren al actief voordat er een patch beschikbaar was). Voor 2025 bedroeg dit cijfer 28,93 %.
- De mediane tijd tussen de publicatie van de CVE en de opname ervan in de KEV-lijst bedraagt 80 dagen, tegenover 120 dagen in 2025.
- In de eerste helft van 2026 werden ongeveer 200 CVE's binnen 31 dagen op de KEV-lijst opgenomen. Dat aantal blijft stabiel ten opzichte van 196 (2024) en 194 (2025), terwijl het totale aantal CVE's sterk is gestegen. Dit weerlegt duidelijk het idee dat alle kwetsbaarheden binnen enkele uren worden uitgebuit.
- VulnCheck waarschuwt uitdrukkelijk voor het 'rijpingsprobleem': voor recente cohorten van CVE's blijft er na verloop van tijd bewijs van misbruik binnenkomen, waardoor de eerste cijfers het misbruik van recente CVE's systematisch onderschatten.

Google Threat Intelligence Group (GTIG): analyse van 2026

De GTIG telde tussen januari en augustus 2026 **141 kwetsbaarheden** die zowel openbaar zijn gemaakt als misbruikt, tegenover 127 in heel 2025. Het maandgemiddelde steeg van 10,5 naar 18.

- Slechts ongeveer 0,23 % van de in 2026 bekendgemaakte kwetsbaarheden werd echter actief misbruikt.
- Die stijging is grotendeels toe te schrijven aan de snelle exploitatie van 'n-days' (recent gepatchte kwetsbaarheden) en niet aan een explosieve toename van het aantal zero-days.
- Het aantal zero-days nam minder sterk toe (gemiddeld van 8 naar 11 per maand) en piekte in augustus.

Mandiant M-Trends 2026 en Verizon DBIR 2026

Uit de incidentresponsgegevens van Mandiant blijkt een geschatte gemiddelde tijd tot exploitatie (TTE, 'time-to-exploit') van -7 dagen. In deze steekproef vond de exploitatie dus vaak plaats vóór de publicatie van de patch. Het is een indicator die aan de patch is gekoppeld en niet de tijd meet tussen de bekendmaking van een CVE en de exploitatie ervan.

Uit het DBIR 2026 van Verizon blijkt dat kwetsbaarheden steeds vaker de toegangsweg zijn bij datalekken (31 % van de lekken) en dat bij tal van aanvalstechnieken steeds vaker AI wordt ingezet. Het rapport stelt echter niet vast dat AI op zichzelf tot een algemene verkorting van de tijd tot exploitatie heeft geleid.

3. Wat we vandaag weten over de mogelijkheden van AI

Het bewijs voor door AI ondersteunde exploitontwikkeling is in 2026 aanzienlijk toegenomen:

- **Mei 2026 | Google**: meldde voor het eerst dat een kwaadwillende actor een zero-day-exploit gebruikte die vermoedelijk met behulp van AI was ontwikkeld.
- **Oktober 2026 | Anthropic**: een intern onderzoeksmodel ontdekte kwetsbaarheden en ontwikkelde meerstaps-exploitketens voor Chrome, Safari, Android, Windows en Linux, waaronder kwetsbaarheden die op afstand kunnen worden uitgebuit en methoden om de sandbox te omzeilen.
- **16 november 2026 | GTIG/Mandiant**: meldde dat kwaadwillende actoren LLM-gebaseerde frameworks gebruiken om het opsporen van kwetsbaarheden, de differentiële analyse van patches en het ontwerpen en uitvoeren van exploits volledig te automatiseren, zonder menselijke tussenkomst en zelfs tijdens inbraken in real time. Daarmee is een kwalitatieve drempel overschreden.

Stand van zaken in november 2026: *„AI verbetert het opsporen van kwetsbaarheden en het ontwikkelen van exploits aanzienlijk en begint in de praktijk bepaalde aanvalsscenario's te verkorten. Tot nu toe is er geen bewijs voor een universeel, door AI aangestuurd exploitatievenster van enkele uren voor alle CVE's. Bij waardevolle doelwitten stellen aanvallers prioriteiten, vooral voor internetgerichte technologieën en randapparatuur. Verdedigers hebben dan mogelijk slechts enkele uren in plaats van meerdere dagen om te reageren."*

4. Wat dit betekent voor verdedigers

De trend is duidelijk en bruikbaar, ook al geeft geen enkel afzonderlijk cijfer de volledige realiteit weer. AI verlaagt de drempel voor het ontwikkelen van exploits. De strategische vraag is niet *„Hoeveel uur hebben verdedigers precies?"*, want het antwoord hangt sterk af van het type kwetsbaarheid, de blootstelling en het profiel van de aanvaller. De echte **vraag** is: „Sporen wij onze kwetsbaarheden op vóór een door AI ondersteunde tegenstander dat doet?"

Precies daarop biedt Hack the Government (HTG) een antwoord. Gecertificeerde ethische hackers, onder wie onderzoekers die actief AI-tools gebruiken, testen overheidssystemen in een wettelijk en gecontroleerd kader. Zo krijgen verdedigers de meest realistische test van hun kwetsbaarheid.

Gecoördineerde melding van kwetsbaarheden is de structurele oplossing.

Of de termijn nu in uren of in maanden wordt gemeten: de organisaties die het best kunnen reageren, hebben al een betrouwbaar proces om meldingen van kwetsbaarheden te ontvangen, te beoordelen en te verhelpen. Het Belgische kader voor gecoördineerde kwetsbaarheidsmelding (CVD), dat sinds december 2022 wettelijk is verankerd, biedt precies die infrastructuur.

5. Belangrijkste bronnen

De volgende bronnen zijn gebruikt bij het opstellen van deze bijlage.

- Cogent Security — Rapport over detectietekortkomingen, 2e kwartaal 2026 (blogartikel)
- Cogent Security — Rapport over detectietekortkomingen, 2e kwartaal 2026 (persruimte / methodologie)
- VulnCheck — Stand van zaken inzake exploitatie in de eerste helft van 2026
- Google Threat Intelligence Group — Trends in het opsporen en misbruiken van kwetsbaarheden in het tijdperk van AI (30 september 2026)
- GTIG/Mandiant — De activiteit van agentgebaseerde bedreigingen overschrijdt een belangrijke drempel (16 november 2026)
- Mandiant — M-Trends 2026
- Anthropic — Ontdekking en misbruik van kwetsbaarheden in kritieke software uit de praktijk met Claude (27 oktober 2026)
- Google — Aanvallers gebruiken AI om kwetsbaarheden te misbruiken, hun operaties te versterken en initiële toegang te verkrijgen
- Verizon — Rapport 2026 over onderzoeken naar datalekken (DBIR)
- CISA — SSVC-gids (het onderscheid tussen een proof of concept (PoC) en een actieve exploitatie)

Deze bijlage is opgesteld door het Centrum voor Cyberveiligheid België (CCB) voor de media ter gelegenheid van het slotevenement „Hack the Government 2026" (25 november 2026). De informatie is bijgewerkt tot en met 19 november 2026.

HACK THE GOVERNMENT 2026

Factsheet: drie edities, tastbare impact en een steeds grotere behoefte

Hack the Government in cijfers

Indicator	1e editie – 2024	2e editie – 2025	3e editie – 2026
Datum van het slotevenement	*27 november 2024*	*26 november 2025*	*25 november 2026*
Totaal aantal deelnemers	*niet beschikbaar*	*71*	*77*
Seniore deelnemers / professionals	*niet beschikbaar*	*39*	*45*
Juniore deelnemers (studenten)	*niet beschikbaar*	*32*	*32*
Ingediende kwetsbaarheidsmeldingen	*154*	*352*	*Te bevestigen (lopend)*
Gevalideerde kwetsbaarheden	*85*	*98*	*Te bevestigen (lopend)*
waarvan kritiek / uitzonderlijk	*7*	*20*	
waarvan hoog	*15*	*12*	
waarvan gemiddeld / laag	*55*	*66*	
waarvan buiten scope, maar gevalideerd	*8*	*9*	
Geteste overheidssystemen / perimeters	*4*	*8*	*12*

Bron: intern rapport van Hack the Government.

Waarom is dit belangrijk? Het tekort aan cybersecuritytalent in België

Hack the Government versterkt niet alleen vandaag de beveiliging van overheidssystemen, maar helpt ook het talent uit te bouwen waar België dringend behoefte aan heeft.

Een **KPMG*-studie uit 2025** over de Belgische cybersecuritysector brengt een uitdaging in kaart die elke deelnemer van nabij kent:

ongeveer 4 000
openstaande vacatures voor cybersecurity in België

44 %
van de organisaties heeft 4 tot 6 maanden nodig om een cybersecurityexpert aan te werven

19 %
van de organisaties heeft 7 tot 12 maanden nodig om de vacature in te vullen

43 %
van de organisaties vindt het aanwerven van cybersecurityexperts moeilijker dan een jaar geleden

1 tot 5
toegewijde cybersecurityspecialisten: dat is de norm voor de helft van de Belgische organisaties

1 op 3
van de organisaties stelt geen enkele vrouw tewerk in cybersecurityfuncties

** Bron: KPMG, Studie over cybersecurity in België (2025), blz. 48–51.*

CENTRE FOR CYBERSECURITY BELGIUM

Hack the Government 2026

Getuigenissen van deelnemers

Ethische hackers aan het woord

DRIE PERSPECTIEVEN

Loopbanen, de community en lessen uit Hack the Government.

01 **Pedro** — PAGINA 2
Zelfstandig consultant in offensieve beveiliging · alias drop
"Zonder de community zou ik vandaag niet staan waar ik nu sta."

02 **Logan** — PAGINA 6
Masterstudent in het laatste jaar
"Leg ook contacten."

03 **Timothy** — PAGINA 7
Bugbountyhunter en ondernemer in cybersecurity
"Je kunt veel leren als je goed luistert naar wat mensen zeggen."

GETUIGENIS 01

Pedro

Zelfstandig consultant in offensieve beveiliging · alias drop

> *"Zonder de community zou ik vandaag niet staan waar ik nu sta."*

1 Kan je jezelf voorstellen en ons kort iets vertellen over je loopbaan? Wat trok je aan in pentesting?

Mijn naam is Pedro, maar in de community rond bug bounty sta ik ook bekend als drop.

Ik ben freelance consultant in offensieve cybersecurity en werk samen met verschillende privébedrijven en overheidsinstellingen. Momenteel ben ik voor een langdurige opdracht aan de slag in de overheidssector als senior pentester.

Het interessante aan mijn parcours is dat ik geen klassieke achtergrond in cybersecurity heb. Oorspronkelijk kwam ik uit de marketing en data science. Maar tijdens de coronaperiode besloot ik enorm veel tijd in cybersecurity te investeren, en uiteindelijk slaagde ik erin om mijn carrière volledig om te gooien.

Ik begon eigenlijk aan de defensieve kant, met digitaal forensisch onderzoek en operationele cyberbeveiliging. Maar diep vanbinnen wist ik vanaf het begin dat ik in offensieve cybersecurity aan de slag wilde.

De uitdaging was om te bewijzen dat ik over de nodige vaardigheden beschikte, zeker zonder een klassieke achtergrond in het vak.

En daar kwam bug bounty in beeld.

Voor mij was bug bounty de ideale manier om te laten zien wat ik in de praktijk kon, in plaats van alleen op certificaten of een cv te vertrouwen.

En eerlijk gezegd is het voor mij daar allemaal echt begonnen. Het heeft zoveel deuren geopend en een enorme rol gespeeld in het uitbouwen van de carrière die ik vandaag heb.

2 Hoe belangrijk is het voor jou om erkend te worden als ethisch hacker? Wat betekent de community van ethische hackers voor jou en voor België?

Voor mij is ethisch hacker zijn in de eerste plaats een manier van denken. En ik denk dat die veel verder gaat dan de technische kant van cybersecurity.

Het gaat om nieuwsgierig zijn, je afvragen hoe dingen werken en problemen oplossen op manieren waar nog niemand aan heeft gedacht.

Het klinkt misschien wat cliché, maar het gaat er letterlijk om buiten de gebaande paden te denken.

Het gaat erom systemen, toepassingen of zelfs processen dingen te laten doen waarvoor ze nooit bedoeld waren, grenzen te verleggen en uiteindelijk de impact aan te tonen of creatieve oplossingen te vinden voor complexe problemen.

En ik denk dat dat ontzettend waardevol is, niet alleen in cybersecurity, maar ook voor de organisaties waarmee we samenwerken.

VRAAG 02 / VERVOLG

En wat de community betreft: voor mij is die alles.

Vóór mijn overstap naar cybersecurity werkte ik in verschillende sectoren, en ik kan oprecht zeggen dat de hackerscommunity iets bijzonders is.

Mensen zijn er ontzettend hartelijk. Ze delen graag hun onderzoek, hun bugs, hun successen, maar ook hun mislukkingen en beperkingen.

En dat waardeer ik enorm.

Zonder de community zou ik vandaag niet staan waar ik nu sta. Het delen van kennis, de samenwerking, de conferenties en alle mensen die ik onderweg heb ontmoet, hebben een enorme rol gespeeld in mijn parcours.

En ik denk dat België een heel sterke en getalenteerde community van ethische hackers heeft, ook al beseffen we dat niet altijd.

Ik ben momenteel trouwens een van de co-kapiteins van het Belgische team dat zal deelnemen aan de nieuwe HackerOne World Cup.

En hopelijk halen we het podium! Dat zou een fantastische prestatie zijn voor de Belgische hackerscommunity.

3 Hoe ben je bij Hack the Government terechtgekomen?

Ik hoorde voor het eerst over Hack the Government tijdens BruCON in 2024.

En ik weet nog dat ik dacht: “Wacht eens, de overheid hacken? Legaal? Dat is een kans die ik niet mag missen!”

Dus besloot ik natuurlijk meteen om deel te nemen.

Het was de allereerste editie, wat het nog spannender maakte.

Voor mij was het de ideale kans om mezelf uit te dagen, mijn vaardigheden te meten met die van andere getalenteerde hackers en te zien waar ik stond tegenover mijn vakgenoten.

Ik was ook benieuwd hoe andere hackers dezelfde doelwitten zouden aanpakken en welke soorten kwetsbaarheden ze zouden ontdekken.

En tijdens die eerste editie slaagde ik er echt in om derde te worden, waar ik heel blij mee was!

Het was een geweldige ervaring, zeker omdat ik toen nog mijn reputatie binnen de community aan het opbouwen was.

4 Kan je een bijzonder moment of een anekdote over Hack the Government delen?

O, zeker!

Ik denk dat het meest memorabele moment voor mij was toen ik de munt van het evenement rechtstreeks van de Belgische premier kreeg.

Dat was toch wel heel bijzonder!

Ik weet nog hoe trots ik op dat moment was. Ik bleef de foto aan mijn collega’s, vrienden en familie tonen.

VRAAG 04 / VERVOLG

Ik bedoel, hoe vaak kan je zeggen dat je legaal overheidssystemen hebt gehackt en daarna een munt van de premier hebt gekregen?

Het is in elk geval een geweldige manier om een gesprek te beginnen!

En los van de erkenning was het ook een heel mooi moment, omdat het liet zien dat ethisch hacken serieus werd genomen en op zo'n hoog niveau werd erkend.

Dat betekende echt veel voor mij.

5 Wat heeft Hack the Government je bijgebracht, en heeft het invloed gehad op wat je daarna hebt gedaan?

Ik zou zeggen dat zichtbaarheid en geloofwaardigheid tot de belangrijkste dingen behoren die Hack the Government mij heeft gegeven.

In die fase van mijn carrière probeerde ik nog mijn plaats te vinden in offensieve cybersecurity.

En deelnemen aan zo'n evenement, zeker als je op het podium eindigt, was een geweldige manier om mijn vaardigheden te tonen en te laten zien dat ik wist waarmee ik bezig was.

Het gaf me ook de kans om veel interessante mensen te ontmoeten, contacten te leggen en zichtbaarder te worden binnen de Belgische cybersecuritycommunity.

En ik geloof oprecht dat die zichtbaarheid mij heeft geholpen om uitgenodigd te worden als spreker op conferenties, deel te nemen aan evenementen met live hacking en later andere kansen te krijgen.

Natuurlijk was dat niet de enige reden waarom die kansen zich voordeden, maar het heeft zeker geholpen om deuren te openen.

Als ik erop terugkijk, was Hack the Government voor mij dus veel meer dan alleen een hackingwedstrijd. Het was ook een belangrijke stap in mijn professionele parcours.

6 Wat maakt Hack the Government vandaag nog waardevol voor jou?

Vandaag ligt de waarde voor mij een beetje anders, zou ik zeggen.

Natuurlijk geniet ik nog altijd van de technische uitdaging en de competitie. Dat zal altijd deel uitmaken van wie ik ben.

Maar wat ik nu het meest waardeer, is het communityaspect.

Het is een kans om vertrouwde gezichten terug te zien, nieuwe mensen te ontmoeten, ideeën uit te wisselen en er gewoon van te genieten dat je omringd bent door mensen die dezelfde passie delen.

Ik vind het ook geweldig om nieuw talent te ontdekken.

Er zijn ontzettend getalenteerde hackers die nog maar net aan hun parcours beginnen, en evenementen zoals Hack the Government geven hen de kans om te laten zien wat ze kunnen.

En wie weet? Misschien sluiten sommigen van hen zich later aan bij het Belgische HackerOne-team, of gaan we ooit zelfs samenwerken.

Je weet nooit waar die contacten toe kunnen leiden, toch?

Dat is een van de dingen die ik zo fijn vind aan deze community.

7 Welk advies zou je geven aan iemand die deelneemt aan Hack the Government 2026?

Geniet om te beginnen zoveel mogelijk van de ervaring!

Hack the Government is een fantastische kans, niet alleen om kwetsbaarheden te vinden, maar ook om bij te leren, mensen te ontmoeten en deel uit te maken van de community.

Doe dus mee aan de discussies op Discord, praat met andere deelnemers en haal zoveel mogelijk uit het evenement zelf.

Mijn tweede advies zou zijn om samen te werken en je echt te concentreren.

Als je op een goede plaats in het klassement mikt, kunnen die twee weken behoorlijk intens worden. Je moet dus het juiste evenwicht vinden tussen diepgaand onderzoek en voldoende pauzes nemen om scherp te blijven.

En dit zou ik vooral minder ervaren deelnemers aanraden: spring niet om de paar minuten van het ene doelwit naar het andere.

Kies liever één toepassing met veel functionaliteiten, neem de tijd om echt te begrijpen hoe die werkt en ga de diepte in.

Begrijp de bedrijfslogica, verken de functies en zoek naar dingen die zich niet gedragen zoals ze zouden moeten.

Daar vind je vaak de echt interessante bugs.

En wie weet? Misschien ontdek je iets dat belangrijk genoeg is om tijdens je eerste show-and-tellsessie te presenteren!

Maar leg jezelf vooral niet te veel druk op.

Of je nu eerste, laatste of ergens daartussen eindigt, je gaat sowieso veel bijleren.

Blijf nieuwsgierig, werk samen, daag jezelf uit en maak vooral plezier. Daar draait hacken om.

> *Zonder de community zou ik vandaag niet staan waar ik nu sta.*
>
> Pedro

GETUIGENIS 02

Logan (Het perspectief van een student)

Masterstudent in het laatste jaar

1 Kan je jezelf voorstellen en kort iets vertellen over je parcours? Wat trok je in eerste instantie aan in pentesting?

Ik ben nog student en zit momenteel in het laatste jaar van mijn master, maar ik leverde bijna twee jaar geleden al een bijdrage aan het CVDP. Nu combineer ik mijn master met bug bounty en doe ik onder meer ervaring op met AI bij beveiligingstests. Hacken en pentests uitvoeren deed ik altijd al, ook toen ik nog veel jonger was. Mijn eerste reflex is om manieren te zoeken om een systeem te 'slim af te zijn' of te 'misleiden'. Ik probeer de grenzen ervan af te tasten.

2 Hoe belangrijk vind je het om als 'ethische hacker' erkend te worden? Wat betekent de gemeenschap van ethische hackers voor jou en voor België?

Heel belangrijk. Dat we in België richtlijnen kunnen volgen, eigenlijk zowat alles kunnen hacken en daar erkenning voor krijgen, is geweldig en uniek in de wereld. Het is ook een fantastische manier om je vaardigheden te testen en bij te dragen aan de veiligheid van België, terwijl je zelfs rechtstreeks je eigen gevoelige gegevens beschermt.

3 Wat bracht je bij Hack the Government?

Het ontdekken van kritieke kwetsbaarheden in systemen van de federale overheid en het melden ervan via het CVDP.

4 Kan je een herinnering of anekdote over HTG delen? Wat heb je ervan meegenomen en heeft het beïnvloed wat je daarna deed? Wat blijft vandaag waardevol voor je?

Ik kwam iemand tegen die ik lang geleden had leren kennen op Nederlandstalige Minecraft-servers. Ik herkende zijn naam en was stomverbaasd toen ik ontdekte dat hij er ook was. We raakten opnieuw aan de praat over onze Minecraft-tijd, over wat we nu doen en hoe we hier allebei terecht waren gekomen.

Ook wat ik daarna deed, is er zeker door beïnvloed: ik nam deel aan evenementen die door de Belgische HackerOne-ambassadeurs werden georganiseerd. Een van hen, dr0p, was ook bij HTG aanwezig. Uiteindelijk hielp dat me om contacten te leggen en bugs te vinden die ik anders niet had gevonden.

5 Wat zou je jongere deelnemers aanraden om volop van HTG 2026 te genieten?

Geniet ervan, doe je best en vind een paar kwetsbaarheden, ook als ze al eerder gemeld zijn. Slaap minder, deel ideeën en informatie op Discord: uiteindelijk zullen mensen je tijdens het fysieke evenement herkennen of op je afstappen en weten wie je bent.

Leg ook contacten. De Belgische hackerswereld is niet *zo* groot: iedereen kent er zowat iedereen. Dit is dus een mooie kans om mensen te leren kennen.

GETUIGENIS 03

Timothy

Bugbountyhunter en ondernemer in cybersecurity

1 Kan je jezelf voorstellen en kort iets vertellen over je parcours?

Ik heet Timothy. Ik ben al op jonge leeftijd met cybersecurity begonnen en was er al behoorlijk in thuis toen ik op mijn 16e voor het eerst aan Hack the Government deelnam. Sindsdien doe ik aan bug bounty en responsible disclosure, help ik bedrijven van elke omvang om hun beveiliging te verbeteren en heb ik twee keer kwetsbaarheden via het CVDP gemeld. In juni van dit jaar ben ik mijn eigen cybersecuritybedrijf gestart. Wat me van bij het begin in pentesting aantrok, is eenvoudig: ik vind het leuk om uit te zoeken hoe systemen werken en hoe ze kunnen falen.

2 Hoe belangrijk vind je het om als 'ethische hacker' erkend te worden?

Voor mij is ethisch hacken de legale manier om te doen wat ik het liefst doe. Dat ik er andere mensen mee help, maakt het nog beter. Elke kwetsbaarheid die ik meld, is er natuurlijk een die niet door iemand met kwade bedoelingen kan worden misbruikt. Voor België tonen evenementen als HTG volgens mij aan dat hackers en de overheid kunnen samenwerken in plaats van elkaar tegen te werken. Zo bouw je aan een betere beveiliging.

3 Wat bracht je bij Hack the Government?

Een vriend raadde het me aan. Bij de eerste editie waren er meer plaatsen vrij dan nu, waardoor ik de kans kreeg om mee te doen, ook al was ik nog jong.

4 Kan je een herinnering of anekdote over HTG delen?

Eerlijk gezegd liep mijn eerste jaar niet zo goed. Ik had nauwelijks iets gevonden en dat was een beetje een realitycheck. Maar in plaats van op te geven, bleef ik leren en kwam ik terug. Vorig jaar ging het een pak beter (7e in het algemeen klassement, geloof ik), en ik hoop dat het dit jaar nog beter gaat. Wat ik ervan heb meegenomen, is dat resultaten niet meteen komen. Je groeit door mee te doen, te leren uit wat niet werkte en opnieuw te proberen. Die ingesteldheid heeft er in grote mate toe bijgedragen dat ik serieus met bug bounty aan de slag ben gegaan en uiteindelijk mijn eigen bedrijf heb opgericht.

5 Wat zou je jongere deelnemers aanraden om volop van HTG 2026 te genieten?

Heb geduld. Bij bug bounty is geduld cruciaal. Laat je niet ontmoedigen als je op de eerste dag niets vindt, of zelfs tijdens je hele eerste editie: dat is mij ook overkomen. Staar je ook niet blind op geavanceerde exploitatietechnieken (en raak niet ontmoedigd als ze niet werken). Sommige van de beste bugs zijn eenvoudige fouten in de logica: zorg dat je begrijpt hoe de applicatie hoort te werken en denk vervolgens na over manieren waarop ze misbruikt zou kunnen worden. En vooral: geniet ervan en praat met de mensen om je heen. Je kunt veel leren als je goed luistert naar wat mensen zeggen.