

Hack The Government (HTG) 2025

Veelgestelde vragen

Wat is een 'ethische hacker'?

Oorspronkelijk hielden “hackers” zich bezig met nieuwsgierig experimenteren en het verkennen van mogelijkheden - zowel op technisch als conceptueel vlak. Na verloop van tijd verschoof hun focus steeds meer naar IT en technologie. In wezen zijn het moderne uitvinders die gepassioneerd zijn door ontdekken en innoveren.

Het concept van een “ethische hacker” is nauw verweven met IT-beveiliging. Het verwijst naar gespecialiseerde “kwetsbaarheidsjagers”, experts die als centrale missie hebben om kwetsbaarheden in IT-systemen bloot te leggen. Het cruciale verschil zit in hun benadering: constructief, transparant en volledig binnen de wettelijke kaders.

Waarom is hun werk belangrijk op het gebied van cyberbeveiliging?

De meest kritieke risico's in een IT-systeem zijn:

- Bekende, onopgeloste kwetsbaarheden
- Onbekende kwetsbaarheden (zogenoemde 'zero-day'-kwetsbaarheden)

Het is een kwestie van tijd en aanpak. Bij bekende kwetsbaarheden zullen routinematige beveiligingsaudits het probleem identificeren en oplossen (“patching” in technisch jargon).

Bij onbekende kwetsbaarheden is snelheid cruciaal. Kwaadwillende actoren kunnen snel misbruik maken van een systeemfout, met potentieel verwoestende gevolgen zoals verstoring van productieprocessen of kritieke diensten.

Bovendien is de technologische realiteit vandaag zo snel dat het misbruiken van zero-day kwetsbaarheden vaak minder dan 24 uur duurt.

Wat is de rol van het CCB?

Het Centrum voor Cybersecurity België (CCB) heeft een heldere, laagdrempelige procedure voor mensen die beveiligingsproblemen in software of IT-diensten ontdekken.

Hoe werkt dat?

Iedereen kan een beveiligingslek melden, zelfs als de betrokken organisatie geen formeel meldingsprogramma heeft. Enkele richtlijnen:

Voor ontdekkers van kwetsbaarheden:

- Handel altijd te goeder trouw

- Vermijd elke vorm van kwaadwillige intentie
- Beperk je acties tot wat strikt noodzakelijk is voor het aantonen van het probleem
- Breng de organisatie en het CCB onmiddellijk op de hoogte

Wettelijke bescherming:

- Volg je bovenstaande richtlijnen, dan ben je wettelijk beschermd
- Je acties worden beschouwd als constructief en verantwoordelijk

Wat is “Hack the Government”?

HackTheGovernment2025 is een initiatief van het Centrum voor Cybersecurity België (CCB) dat de digitale veiligheid van Belgische overheidsdiensten wil versterken.

Ethische hackers worden uitgenodigd om de IT-systemen van specifieke overheidsinstellingen te toetsen, met als enige doel kwetsbaarheden op een verantwoorde manier te identificeren en te rapporteren. Het gaat verder dan een wedstrijd - het is een gezamenlijke oproep tot samenwerking tussen alle betrokkenen, gericht op verhoging van de nationale cyberveiligheid.

Waarom is dit belangrijk?

Dit proces maakt digitale beveiliging krachtiger door samenwerking en ethische verantwoordelijkheid centraal te stellen. In plaats van een repressieve aanpak worden professionals aangemoedigd om constructief bij te dragen aan de collectieve digitale veiligheid.

Samenvatting: Dit initiatief mobiliseert getalenteerde experts om kwetsbaarheden in overheids-IT-systemen bloot te leggen. Door proactief zwakke plekken te identificeren, kunnen we vooruit zijn op potentiële cyberaanvallen. Het is een strategische benadering die niet alleen overheidsinstanties beschermt, maar uiteindelijk ook de veiligheid van alle burgers waarborgt.