



CULTUUR

Cybersecurity
Competitie voor
kampioen die
hackt zonder AI

CULTUUR 4-5

REPORTAGE HACKINGCOMPETITIE • Op de twaalfde European Cybersecurity Challenge financierde de EU deze week een competitie met ruim 400 getalenteerde hackers. Die zijn hard nodig in het licht van de recente golf cyberaanvallen, waarbij vaak AI wordt gebruikt. Maar dat is tijdens deze hackingcompetitie in Bochum juist níét toegestaan.

Door **Pippen Sardjoe**

Een dag lang proberen ze elkaars server te hacken

Vlaggen over de tribunes en om schouders, elk jaar een ander Europees gastland, een gemoeidelijke sfeer: de European Cybersecurity Challenge heeft wel wat weg van het Eurovisie Songfestival. Maar dan met minder glitter en meer hoodies en opengeklapte pizadozen tussen laptops. In de grote hal van het congrescentrum in het Duitse Bochum zitten de cybertalenten de hele dag gebogen over hun laptops aan de teamtafels. Deze zijn bedolven onder lege blikjes Red Bull en flessen Club-Mate.

In Bochum vond deze week de twaalfde editie van de hacking-competitie plaats, die wordt gefinancierd door de Europese Unie om getalenteerde hackers bij elkaar te brengen. Gedurende drie dagen streken ruim vierhonderd jongeren tussen de 14 en 25 jaar in nationale teams om het Europese kampioenschap. In totaal waren vijfendertig Europese landen en zeven gastlanden vertegenwoordigd. De tienkoppige teams zijn samengesteld via nationale selectiewedstrijden, waar meer dan 30.000 deelnemers aan hebben meegedaan.

De ECSC is een *Capture The Flag*-competitie (CTF), waarbij deelnemers punten verdienen door uiteenlopende puzzels tot een goed eind te brengen, van het oplossen van cryptografische problemen tot het opsporen van fouten in websites. In tegenstelling tot *hackathons*, die vaak een commerciële inslag hebben en een product (software of een app) moeten opleveren, draait een CTF om het spel zelf. Tegelijkertijd helpen zulke competities om de volgende gene-

ratie cyberexperts op te leiden, die in het licht van steeds frequentere en geavanceerdere cyberaanvallen hard nodig zijn.

Op donderdag, de laatste competitiedag, spelen de teams *Attack-Defense*. Van elf uur 's ochtends tot zeven uur 's avonds verdedigen ze hun eigen servers en vallen ze die van andere landen aan. Jonathan Jagt (23), aanvoerder van het Nederlandse team, kijkt tevreden terug op het verloop: „We hebben snel gereageerd en hebben zo punten naar binnen kunnen hengelen. Ik ben heel trots, we hebben geen enkele aanval erdoor laten gaan.”

Afgezien van kort overleg met teamgenoten en de aanvoerders houden de deelnemers gedurende de dag hun ogen gericht op hun monitoren. Een groot scherm in de hal toont afwisselend het scorebord en een landkaart waarop de aanvallen live te volgen zijn. Een verrassende aanval of een plotse-linge puntensprong levert applaus van de deelnemers op.

AI is niet toegestaan

Tussen de tafels lopen toezichthouders rond, de zogeheten *watchdogs*, die de twee belangrijkste regels van de competitie handhaven: de opdrachten mogen niet worden gedeeld met buitenstaanders en er mag geen gebruik worden gemaakt van Large Language Models (LLMs), oftewel AI.

Bill Gates stelde in een recente podcast van de *New York Times* dat AI een gouden tijdperk voor hackers heeft ingeluid. In slechts een fractie van de tijd kunnen zogeheten AI-agenten (autonome softwareprogramma's) het werk doen waar experts voorheen uren hun hoofd over braken. Maar bij CTF is dat laatste juist de lol, legt Per

Schrijver (22) uit. De student van de TU Delft deed eerder mee aan de ECSC en loopt dit jaar rond als *watchdog*. Voor de competitie liet hij hartjes en de letters CTF in zijn haar verven. „Ik geef de voorkeur aan competities waar geen LLMs zijn toegestaan. Het gaat om de denkpuzzels die je zelf wilt oplossen.”

„Je ziet dat AI heel erg de CTF-sport aan het veranderen is, of misschien wel aan het verpesten”, vertelt Michiel Oosterwijk (60), oprichter en bestuurslid van Stichting Challenge The Cyber. De stichting organiseert de jaarlijkse Nederlandse deelname aan de ECSC. Vorig jaar mochten deelnemers nog AI gebruiken, maar de ontwikkelingen gaan dusdanig snel dat de ECSC-organisatie heeft besloten het gebruik ervan dit jaar te ver-

bieden. „AI zou waarschijnlijk alle opdrachten heel snel oplossen”, zegt Oosterwijk.

Bij sommige CTF-competities, zoals de International Cybersecurity Challenge waar continenten als teams meedoen, mag AI wel worden gebruikt, maar alleen binnen een budget dat vooraf is vastgesteld. „Anders wordt het *pay to win*: degene die de duurste AI kan inzetten wint”, vertelt Yannik Marchand (26). Hij is ook oud-deelnemer en zit dit jaar in de organisatie. Vier van de opdrachten van dit jaar heeft hij geprogrammeerd.

„Het is allebei relevant”, zegt hij, terwijl hij naar de deelnemers-tafels kijkt. „Zowel de AI-skills opdoen als zelf de problemen nog kunnen oplossen. Misschien dat er in de toekomst wel twee competities komen.”

Waar voorheen ervaring in cybersecurity bij CTF-competities bepalend was, zijn dat nu dure AI-tools, vertellen Simon Tulling (27) en Rick de Jager (27), de coaches van het Nederlandse team. De Jager: „Het mooie van dit soort cyberwedstrijden was dat je de vaardigheden die je ontwikkelt één op één nodig hebt om een goede carrière in cyber voor jezelf op te bouwen. Door de nieuwe techniek is het verschil tussen maar één jaar en vijf jaar ervaring een beetje weg.”

Vrijwel geen vrouwen

Behalve kort overleggen met de aanvoerder mogen de coaches gedurende de competitiedag zelf weinig doen, dus houden ze voornamelijk het scorebord in de gaten. Het Nederlandse team is dit jaar relatief jong, met onder ande-



Nederlandse deelnemers aan de European Cybersecurity Challenge. FOTO ANP/DPA

re een deelnemer van vijftien en twee van zestien jaar oud. Eén van de zestienjarigen is een meisje, verder bestaat het team volledig uit jongens en mannen. Maar weinig delegaties hebben meisjes of vrouwen in het team.

Nederland doet sinds 2019 mee aan de ECSC. „We kregen in 2018 het verzoek van ENISA, het EU-agentschap voor cyberveiligheid, om een nationale competitie te organiseren zodat we aan de Europese finale mee konden doen”, vertelt Oosterwijk, die tevens werkt bij het NCSC, het Nederlandse expertisecentrum voor digitale veiligheid. „We zagen de mogelijkheden om jongeren te stimuleren cybersecurity-skills te ontwikkelen. En vooral ook om te zorgen dat jongeren die dit in hun vrije tijd doen, dit positief gaan inzetten.

Doel van de challenge: de elite van cybersecurity bij elkaar brengen om zo van elkaar te leren

En dat ze niet door criminelen worden opgepikt, want dat gebeurt.”

De recente hacks en cyberaanvallen - waarbij in veel gevallen AI een rol speelde, zoals bij het Amerikaanse AI-bedrijf Hugging Face, de banken in Zuid-Korea en een Australische overheidssite - onderstrepen de kwetsbaarheid van digitale infrastructuur in het AI-tijdperk. „Je ziet de effecten van de hacks en ransomware-operaties

duidelijker terug in je normale leven”, zegt coach De Jager. „Met de Albert Heijn en Odido is het heel dichtbij”, vult Tulling aan.

Twee weken terug werd ‘whizz-kid’ Pepijn van der S. opgepakt op verdenking van deelname aan ShinyHunters, het hackerscollectief achter de aanval op Odido waarbij in februari gegevens van miljoenen Nederlandse klanten werden gestolen. Tulling: „Met die jongen van ShinyHunters zag je dat hij nergens bij ons bekend was. Hij had ook CTF's kunnen doen in plaats van wat hij uiteindelijk heeft gedaan.”

Europees talent werven

Opvallend is dat ondanks al het jonge cybertalent er bij de competitie nauwelijks bedrijven aanwezig zijn, los van de hoofdsponsors. „Werven zie je meer bij *hackathons*”, licht Oosterwijk toe.

Overigens heeft ieder nationale team wel zijn eigen sponsors. Oosterwijk wijst naar de logo's op zijn team-NL-vest: de cybersecuritytak van Bureau Veritas, IT-stichting Competens en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

„Het doel van de competitie is om de top van de elite cybersecurity bij elkaar te brengen zodat ze van elkaar kunnen leren”, vertelt Evangelos Ouzounis (56) van ENISA. Naast het bevorderen van een gemeenschap „mist Europa bovendien cybersecurityprofessionals, er is een gat van 300.000 mensen”. Het bedrijfsleven en criminele actoren beschikken over meer geld, benadrukt Ouzounis, maar „je hoopt dat de deelnemers hier er uiteindelijk voor kiezen om overheidsinstanties te helpen”.

Aan de European Cybersecurity Challenge doen vrijwel alleen **jongens en mannen** mee. FOTO ANP/DPA

