

L'UNIVERSITÀ DI PISA VINCE CYBERCHALLENGE.IT, LA GARA NAZIONALE DEGLI HACKER ETICI

Roma, 3 ottobre 2020

Dopo ore di sfide informatiche e due giorni di eventi, si è conclusa la quarta edizione di CyberChallenge.IT, la gara nazionale degli **hacker etici** italiani. Per la prima volta interamente online, a causa della complessa emergenza sanitaria che stiamo vivendo, l'evento ha coinvolto **560 ragazzi tra i 16 e i 23 anni**, per un totale di 28 squadre, che rappresentano 26 università, il Centro di Competenza Cybersecurity Toscana e il Comando per la Formazione e Scuola di Applicazione dell'Esercito di Torino. Organizzata ogni anno dal Laboratorio Nazionale di Cybersecurity del CINI (Consorzio Interuniversitario Nazionale per l'Informatica), l'iniziativa costituisce il maggiore sforzo di formazione nazionale nell'ambito della cyber security, nonché uno **dei più riconosciuti a livello europeo**. A conquistare il primo gradino del podio, per questa edizione, è stata l'**Università di Pisa**. Seguono il **Politecnico di Milano** al secondo posto e l'**Università degli Studi di Verona** terza classificata.

I team si sono confrontati in una complessa gara di tipo *Capture the flag* (Ctf), una sorta di ruba bandiera virtuale, nella quale ciascuna squadra è stata chiamata ad **attaccare** le infrastrutture informatiche degli avversari, **proteggendo** al contempo la propria, e impedendo ad altri di prenderne il controllo. Uno dei campi di battaglia, creato apposta per l'occasione, è stato il nuovo cyber range *Paideusis*: un'infrastruttura permanente, fisicamente ospitata a Torino dalla Fondazione Links, che l'ha realizzata insieme al Laboratorio Nazionale di Cybersecurity e con la collaborazione tecnica dell'azienda canavese Tiesse. Tutta contenuta in una sola stanza, *Paideusis* consiste in un ambiente fisico accessibile in remoto nel quale interagiscono tra loro i modem di ciascun team: pur se tutti i partecipanti giocheranno da remoto, dalle loro università o addirittura da casa, sarà in questo spazio fisico che perverranno i loro comandi e che - materialmente - si svolgerà la gara.

Questo tipo di competizione richiede **ampie competenze** e una squadra eterogenea per formazione, in grado di esercitare tecniche offensive e difensive nell'ambito della cifratura, della gestione dei server, e dell'analisi di codice sorgente.

Tutti temi che i ragazzi di CyberChallenge.IT hanno approfondito durante il percorso di **formazione altamente specializzata** in sicurezza informatica, della durata di **dodici settimane**, al quale hanno partecipato tra marzo e maggio. Tra gli argomenti affrontati durante i corsi di formazione, organizzati dalle ventotto sedi nazionali con il coinvolgimento di esperti esterni e aziende, particolare attenzione è stata data alla sicurezza delle infrastrutture informatiche e dell'hardware, alla web security, alla protezione delle telecomunicazioni e alle capacità di attacco e difesa di un sistema informatico. Ciascun tema rappresenta un diverso punto critico del mondo digitale e tutti concorrono alla maggiore capacità di protezione sia delle aziende sia dell'intero "Sistema Paese", già oggetto in Italia della legge sul perimetro di sicurezza nazionale cibernetica.

Nel secondo giorno di CyberChallenge.IT, le otto squadre che si sono maggiormente distinte durante la gara Ctf hanno esposto delle **presentazioni** legate al mondo della sicurezza digitale. Scopo di questo segmento di gara è di mettere alla prova le capacità divulgative degli hacker etici, che sempre più spesso dovranno fare i conti con la centralità della materia anche nelle vite dei non addetti al settore, che quotidianamente si confrontano con l'esigenza di un maggiore controllo delle proprie operazioni informatiche, in difesa di sé stessi e delle organizzazioni con cui lavorano. Al "tavolo" della giuria (che ovviamente ha preso parte all'evento in remoto), si sono seduti esperti della sicurezza, della divulgazione scientifica e un rappresentante per ciascuna delle aziende sponsor Platinum (Accenture, Aizoon, Blu5 Group, Eni, Exprivia, IBM, KPMG, Leonardo, Ntt Data, Numera, Telsy) che ogni anno permettono la realizzazione dell'evento. A

loro si aggiungono anche gli sponsor Gold (BIP, Cisco, Banca Monte dei Paschi di Siena, NEGG, Novanext, PwC) e Silver (Digi-One, ICT Cyber Consulting), che costituiscono l'indispensabile contributo che ogni anno permette a oltre 500 ragazze e ragazzi di partecipare a CyberChallenge.IT.

Nazionale Italiana di Cyberdefender

Il prossimo passo nelle attività del Laboratorio Nazionale di Cybersecurity sarà la **convocazione** dei giovani che si sono maggiormente distinti durante le gare per l'ingresso nel TeamItaly: la nazionale italiana di esperti di sicurezza informatica che **ogni anno rappresenta l'eccellenza del Paese** nelle competizioni nazionali. Il prossimo appuntamento sarà a novembre, con un'amichevole a livello europeo organizzata dall'Agenzia europea per la sicurezza delle reti e dell'informazione (Enisa), che sostituisce il campionato europeo (European Cybersecurity Challenge - Ecsc), rimandato a causa del Covid-19. Resta quindi - d'ufficio - sul podio europeo anche la nazionale italiana, che a Ecsc19 aveva conquistato il secondo posto.

Talento e competenza dei giovani esperti nazionali di sicurezza informatica sono riconosciuti anche a livello nazionale: il 7 febbraio di quest'anno, ad Ancona, il vicedirettore generale del Dipartimento di Informazione per la Sicurezza (Dis), Roberto Baldoni, ha premiato il TeamItaly di fronte a una platea di istituzioni accademiche e rappresentanti politici e militari. L'anno precedente, a ITASEC19, la cerimonia di premiazione ha visto la partecipazione dell'allora ministro italiano della Difesa, Elisabetta Trenta.

"Vedere la gara nel vivo, pur da remoto, è stata la più grande soddisfazione dopo mesi di lavoro nel quale abbiamo fatto i conti, come tutti, con una pandemia globale", ha commentato Paolo Prinetto, direttore del Laboratorio Nazionale di Cybersecurity. "Questa è la più significativa dimostrazione di come, pur con 560 ragazzi e ben 28 istituzioni coinvolte, ogni problema può diventare opportunità, quando la motivazione è forte e rivolta alla cultura della sicurezza e del progresso tecnologico. Ci sono tutte le basi per crescere ancora e - speriamo - per poter realizzare la prossima CyberChallenge.IT in presenza".

Che cos'è il Laboratorio Nazionale di Cybersecurity - CINI

Il Laboratorio Nazionale di Cybersecurity del CINI coordina attività di ricerca, sviluppo e formazione sui temi della sicurezza informatica a livello nazionale e internazionale per aiutare il sistema paese a essere più resiliente alle minacce cibernetiche. Il Laboratorio si impegna quindi a migliorare le misure di protezione della pubblica amministrazione e delle imprese da attacchi informatici supportando anche i processi di definizione degli standard e dei framework metodologici a livello nazionale. <https://cybersecnatlab.it/>

<https://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it