Progetto CyberChallenge.IT

Presentazione

Indice

1. Introduzione

CyberChallenge.IT è un progetto del Laboratorio Nazionale di CyberSecurity del CINI che punta a scoprire e valorizzare il talento "cyber" nascosto in giovani fra 16 e 22 anni che studiano sul territorio italiano.

Il progetto mira a identificare giovani talenti e, in prospettiva, a ridirezionare parte della workforce verso tematiche di grande rilevanza per il sistema Paese e nelle quali è noto esservi una enorme carenza di competenze a livello planetario.

Come obiettivo correlato, l'iniziativa punta a formare giovani per la *Squadra Nazionale di Cyberdefender* che parteciperà alla European Cybersecurity Challenge (ECSC)[1] che si svolge con cadenza annuale.

L'edizione 2018 di CyberChallenge.IT proporrà corsi di addestramento riservati a studenti brillanti svolti presso dieci sedi universitarie italiane distribuite su tutto il territorio nazionale e culminerà nel *primo campionato italiano Capture-The-Flag (CTF) in cybersecurity*.

1.1 L'esperienza del pilot 2017 presso Sapienza Università di Roma

Il pilot CyberChallenge.IT, sperimentato nel 2017 presso Sapienza Università di Roma, ha riscosso notevole interesse tra i giovani, la stampa, le aziende e il governo nazionale. L'evento, seppur limitato al solo ateneo romano, ha ricevuto 700 domande di partecipazione e numerose richieste di estensione ad altre città italiane da parte di giovani interessati.

L'iniziativa è stata seguita costantemente dalla stampa e la cerimonia di premiazione finale è stata presieduta dal Direttore del Dipartimento delle Informazioni per la Sicurezza (DIS), Prefetto Alessandro Pansa.

Il Ministero per lo Sviluppo Economico (MISE) ha affidato al Laboratorio Nazionale di Cybersecurity del CINI, in qualità di organizzatore di CyberChallenge.IT, il compito di formare la Squadra Nazionale di Cyberdefender che nell'ottobre 2017 ha partecipato per la prima volta alla ECSC, **conquistando il terzo posto** (a pari merito con UK), su 15 nazioni partecipanti.

1.2 L'iniziativa 2018 estesa a tutto il paese – Sedi partecipanti

In questo quadro, il lancio dell'iniziativa su scala nazionale si prospetta come un'occasione unica per gli atenei italiani per attrarre studenti brillanti, rafforzare i contatti con le aziende e il governo, e incrementare la propria visibilità mediatica in operazioni socialmente rilevanti e di impatto per il grande pubblico.

L'iniziativa CyberChallenge.IT 2018, aperta a tutte le sedi afferenti al Laboratorio Nazionale di CyberSecurity disponibili a condividerne l'organizzazione, vede la partecipazione delle seguenti otto sedi:

- Politecnico di Milano – referente Prof. Stefano Zanero
- Politecnico di Torino – referente Prof. Antonio Lioy
- Sapienza Università di Roma – referente Prof. Camil Demetrescu
- Università Ca' Foscari di Venezia – referente Prof. Riccardo Focardi.
- Università di Genova – referente Prof. Giovanni Lagorio
- Università di Milano – referente Prof. Stelvio Cimato
- Università di Napoli Parthenope – referente Prof. Luigi Romano
- Università di Padova – referente Prof. Mauro Conti

[1] https://www.europeancybersecuritychallenge.eu

1.3 Contesto internazionale

Vi sono numerose iniziative internazionali per promuovere la diffusione di una cultura della cybersecurity facendo leva sulla competizione come stimolo per attrarre giovani talenti. Paesi come UK, Austria, Germania, Svizzera, Spagna, Romania organizzano, da alcuni anni, competizioni nazionali che selezionano i migliori candidati per formare le squadre nazionali che partecipano alla ECSC.

Numerosi team organizzano competizioni Capture-The-Flag (CTF) on-line per gli appassionati[2]. Fra le principali ricordiamo DEF CON (on-site) e iCTF (online).

In ambito italiano ricordiamo polictf[3], organizzata dal Politecnico di Milano e patrocinata dal Laboratorio Nazionale di Cybersecurity del CINI.

1.4 Chi può partecipare

Per l'**edizione del 2018**, le iscrizioni sono aperte per i giovani nella fascia di età compresa tra i 16 e i 22 anni compiuti nel 2017, vale a dire i **nati negli anni 1995-2001**.

Si noti che uno studente in regola con il corso di studi inizia il 4° anno delle scuole superiori all'età di 17 anni (o 16 in caso di anticipo) e completa la laurea triennale all'età di 22 anni (o 21 in caso di anticipo). In generale, gli ammessi saranno studenti che nell'anno 2017/2018 frequentano:

1) un anno scolastico compreso tra il 4° anno delle superiori e il 3° anno della laurea triennale
2) il 1° anno della laurea magistrale (se hanno fatto anticipo)
3) il 3° anno delle superiori (se non hanno fatto l'anticipo).

In merito ai potenziali problemi posti da una classe di studenti con competenze molto diverse (tenendo conto delle diverse età comprese tra i 16 e i 22 anni), è importante evidenziare come l'esperienza del 2017 non abbia rivelato criticità, anche grazie alla rigorosa selezione nella fase di ingresso. Gli studenti più giovani appassionati di programmazione spesso approfondiscono i temi informatici a scuola o per conto proprio. Il più giovane del team CyberChallenge.IT 2017, che aveva precedentemente partecipato alle olimpiadi italiane di informatica, è arrivato primo ai test di ammissione, è stato tra i vincitori della challenge finale ed è stato chiamato a fare parte della Squadra Nazionale Italiana Cyberdefender 2017.

1.5 Svolgimento

L'iniziativa CyberChallenge.IT prevede:

1. un ***test di ammissione*** volto a selezionare studenti con eccellenti capacità logiche, di programmazione e di problem-solving, senza richiedere conoscenze pregresse in cybersecurity. Il test di ammissione si svolge in due fasi: un primo test online consente l'accesso a un successivo test, svolto in presenza presso le varie sedi. La selezione porta a un gruppo di **20 partecipanti** per sede.

2. un ***percorso formativo*** mirato a fornire un'introduzione tecnica ed etica alla cybersecurity e finalizzato all'acquisizione delle competenze richieste per affrontare le competizioni finali CyberChallenge.IT, che ricalcano il formato delle gare CTF classiche.
   Il percorso ha una durata complessiva di circa **70 ore** distribuite su **tre mesi** e sarà svolto presso ciascuna sede in orari compatibili con le attività didattiche degli studenti (es. venerdì pomeriggio/sabato mattina).
   Diversamente da altre competizioni nazionali, in cui i concorrenti si preparano per conto proprio risolvendo challenge pubblicate sul Web, il progetto CyberChallenge.IT punta a facilitare l'accesso alle gare fornendo un **contesto di addestramento intro-**

[2] https://ctftime.org
[3] http://www.polictf.it

duttivo, guidando gli studenti passo-passo nella risoluzione di challenge CTF di complessità via via crescente in un ambiente sicuro, senza assumere alcuna conoscenza pregressa in cybersecurity.

3. una ***gara di qualificazione CTF locale*** per selezionare i migliori team di studenti di ciascuna sede a cui segue una premiazione locale e una recruitment fair in cui gli studenti incontrano gli sponsor.
4. un ***evento nazionale*** a cui partecipano i migliori team di studenti di ciascuna sede e che prevede:
    a. una ***competizione CTF on-site***
    b. una ***cerimonia di premiazione nazionale*** presieduta da rappresentanti delle istituzioni italiane
    c. una ***recruitment fair nazionale***, in cui i migliori talenti cyber italiani incontrano le aziende che sponsorizzano l'evento a livello nazionale.

Durante tutte le fasi dell'iniziativa, tranne che per il test di ammissione, i partecipanti lavoreranno sui propri computer portatili.

1.6 Timeline per l'edizione 2018

4 dicembre	aperture iscrizioni online
20 gennaio	chiusura iscrizioni online
25-27 gennaio	pretest valutazione online
1 febbraio	test di ammissione locale presso ciascuna sede
21 febbraio	pubblicazione elenco degli ammessi
1 marzo–31 maggio	corso di formazione/addestramento CyberChallenge.IT presso ciascuna sede
7-8 giugno	qualificazioni locali e recruitment fair con gli sponsor
27-28 giugno	evento finale nazionale CyberChallenge.IT 2018: • 27 giugno: CTF nazionale • 28 giugno: premiazione e recruitment fair con gli sponsor nazionali
ottobre-novembre	European Cybersecurity Challenge (ECSC'18)

2. Modalità operative

2.1 Iscrizione

I candidati interessati potranno iscriversi tra il 4 dicembre 2017 e il 20 gennaio 2018 sul sito Web www.cyberchallenge.it, compilando un apposito form e specificando, tra l'altro, anche una **sede primaria** ed eventualmente una **sede secondaria** in cui vorrebbero seguire i corsi.

La sede primaria è quella presso la quale in candidato intende svolgere il test in presenza e, se ammesso, il corso stesso. La sede secondaria sarà proposta per seguire il corso nel caso in cui non vi sia più posto nella sede primaria, secondo le modalità discusse nel Paragrafo 2.2.2.

2.2 Test di ammissione

Il **test di ammissione** avverrà in **due fasi:**

1. pre-test on line
2. test in presenza

Tutti i testi delle prove di ammissione saranno in lingua **inglese**.

2.2.1 Pre-test online

Lo scopo del pre-test online, che sarà proposto **giovedì 25 gennaio 2018** in un orario da stabilirsi, è quello di ridurre il numero di candidati ammessi ai test in sede a una quota sostenibile, fornendo al contempo indicazioni utili ai partecipanti sul loro livello di preparazione.

Il pre-test sarà costituito da **quiz** su argomenti di **programmazione in linguaggio C** e di **logica**.

Sulla base dei risultati del pre-test, sarà stilata una **graduatoria** per ciascuna sede, basata sul numero di domande a cui si è risposto correttamente, prediligendo, a parità di risposte corrette, i candidati più giovani.

Per ciascuna sede, saranno **ammessi al test in presenza** i primi della graduatoria del pre-test online in numero variabile a seconda della sede. Si consulti la pagine della sede locale sul sito Web cyberchallenge.it.

2.2.2 Test in presenza presso ciascuna sede

Il test si terrà giovedì 1 febbraio 2018 simultaneamente in tutte le sedi e sarà costituito da due parti:

- **mattina**: test di 1 ora a quiz su programmazione in **linguaggio C** e **logica**, riservato a tutti gli ammessi al test in presenza; a seconda della disponibilità delle aule informatiche, potrà essere necessario svolgere turni multipli.
- **pomeriggio**: prova di programmazione al calcolatore della durata di 3 ore riservata ai primi classificati nella prova a quiz della mattina, in numero variabile a seconda della sede. Per alcuni esercizi, **il linguaggio richiesto è il C**. Per altri invece, più orientati al problem-solving, lo studente sarà **libero di scegliere tra il C e altri linguaggi** come C++, Python o Java (la pagina locale della sede dove si svolgerà il test di ammissione indicherà i linguaggi supportati per lo svolgimento della prova).

Il punteggio ottenuto al test in sede sarà definito come combinazione dei risultati delle due prove della giornata e non dipenderà dal risultato del pre-test.

Ai fini dell'ammissione, sarà stilata una **graduatoria nazionale** basata sul punteggio acquisito nel test in sede, prediligendo a parità di punteggio, i candidati più giovani.

2.3 Formazione delle Classi

Per **formare le classi**, si procederà in ordine di graduatoria: ogni candidato sarà assegnato alla sede primaria indicata, se vi è ancora posto, altrimenti sarà assegnato alla sede secondaria, qualora indicata. In caso di **rinunce**[4] entro domenica 25 febbraio, si riapplicherà l'algoritmo.

Gli eventuali posti generati da rinunce successive al 25 febbraio saranno messi a disposizione, a discrezione della sede, esclusivamente a studenti locali in ordine di graduatoria.

Uno studente ammesso non potrà cambiare sede.

2.4 Percorso formativo

Il *Percorso Formativo* del progetto CyberChallenge.IT mira a fornire un'introduzione tecnica ed etica alla cybersecurity ed è finalizzato all'acquisizione delle competenze richieste per affrontare le competizioni finali, che ricalcano il formato delle gare CTF classiche.

[4] Come scenario tipico, uno studente ammesso su sede secondaria potrebbe decidere di rinunciare per motivi logistici, lasciando il posto a uno studente successivo in graduatoria.

Diversamente da altre competizioni nazionali, in cui i concorrenti si preparano per conto proprio risolvendo challenge pubblicate sul Web, il Progetto CyberChallenge.IT punta a facilitare l'accesso alle gare fornendo un *contesto di addestramento introduttivo*.

Il Percorso Formativo di CyberChallenge.IT guida gli studenti passo-passo nella risoluzione di challenge CTF di complessità crescente, senza assumere alcuna conoscenza pregressa in cybersecurity.

Il Percorso Formativo si articola in due momenti diversi:

- crash course introduttivi e opzionali;
- corso di formazione/addestramento.

2.4.1 Crash course

Si tratta di un insieme di moduli introduttivi e opzionali, della durata di 2-4 ore caduno, fruibili individualmente via Web dai partecipanti e mirati a fornire loro alcune conoscenze di base su temi quali networking e linguaggio Assembler x86.

SI tratta, in pratica, di corsi di *mis-à-niveau* (*crash course*) su tematiche la cui conoscenza è un prerequisito per poter partecipare in modo efficace al corso successivo.

I corsi, in lingua inglese, sono registrati e resi disponibili tramite una delle piattaforme del progetto.

2.4.2 Corso di formazione/addestramento

Si svolgerà in 12 settimane, tra giovedì 1 marzo e sabato 26 maggio 2018 e include:

- lezioni (18 ore): nozioni fondamentali sulla cybersecurity;
- sessioni di addestramento (48 ore): addestramento alle gare CTF.

Lezioni

Si tratta di lezioni introduttive alla sicurezza informatica (***cyber-essential***), organizzati in **12 moduli** di **90 minuti** ciascuno, erogati in incontri settimanali e organizzati in due slot di 45' intervallati da una pausa.

I cyber-essential sono una caratteristica peculiare di CyberChallenge.IT.

Ciascuna lezione consisterà di:

- *slide* in lingua inglese: queste saranno utilizzate dagli istruttori locali per le lezioni in aula;
- *materiale di approfondimento*: sarà scaricabile dagli studenti partecipanti dal portale del progetto;
- *registrazione delle lezioni*: le lezioni saranno scaricabili da una delle piattaforme del progetto sotto forma di file video dagli studenti partecipanti. Esse potranno essere utilizzate come materiale a supporto per le lezioni frontali, in modo del tutto analogo al servizio offerto da alcuni atenei che consente agli studenti di accedere, via streaming, alle registrazioni delle lezioni frontali effettuate in aula;
- *erogazione*, in modalità frontale, delle lezioni relative utilizzando le slide di cui sopra.

I cyber-essential vertono sia su **contenuti tecnici** sia sulla formazione di **soft skill** rilevanti per una carriera in cybersecurity, come la capacità di presentare argomenti tecnici in modo chiaro ed efficace, mettendoli in una prospettiva comprensibile anche a non esperti del settore.

Sessioni di addestramento

Si tratta di 12 sessioni settimanali di 4 ore ciascuna mirate ad addestrare i partecipanti alla risoluzione passo-passo di challenge CTF.

La didattica è erogata in periodi compatibili con le attività scolastiche/universitarie dei partecipanti, ad esempio il sabato mattina o il venerdì pomeriggio, tenendo conto della disponibilità degli spazi dedicati e dell'organizzazione scolastica locale.

Il materiale didattico messo a disposizione dal CINI consiste in un paniere di CTF corredate da write-up che illustrano le soluzioni. Ciascuna sede organizzerà in piena autonomia la scelta delle challenge su cui concentrarsi.

A inizio corso, a ciascun partecipante viene fornito dal CINI un toolkit comune a tutte le sedi con una serie di strumenti di analisi e sviluppo utilizzabili durante l'addestramento.

Organizzazione del calendario per l'edizione 2018

Lezione e sessioni di addestramento si svolgono con cadenza settimanale tra marzo e maggio. Il giorno della settimana è stabilito dalla singola sede, tenendo conto delle festività:

13 feb	Martedì Grasso	**25 apr**	Anniversario della Liberazione
14 feb	San Valentino	**28 apr**	Sa die de sa Sardigna
19 mar	Festa di San Giuseppe	**1 mag**	Festa dei Lavoratori
25 mar	Le Palme	**9 mag**	Giorno Europeo
25 mar	Ora Legale	**13 mag**	Festa della Mamma
1 apr	Pasqua	**20 mag**	Pentecoste
2 apr	Lunedì dell'Angelo	**21 mag**	Lunedì di Pentecoste

2.5 Eventi CTF finali

Ciascuna edizione prevede un evento finale locale presso ciascuna sede (nel seguito "Evento CTF locale") e un evento nazionale finale (nel seguito "Evento CTF nazionale"). Gli eventi finali si svolgono su due giorni e prevedono:

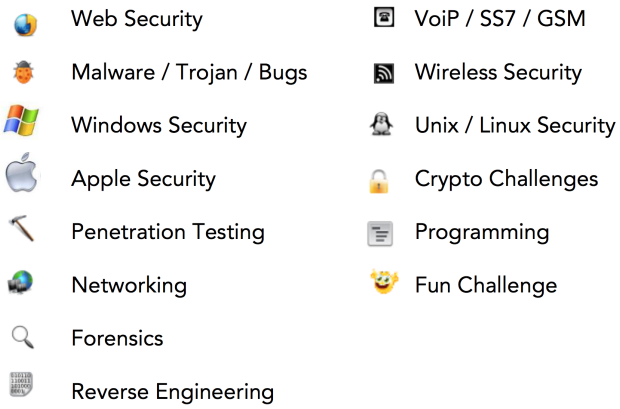
- una competizione CTF
- presentazioni dei concorrenti che illustrano le soluzioni delle CTF svolte
- una cerimonia di premiazione
- un recruitment fair in cui i partecipanti incontrano le aziende.

Stili di gara.

Le CTF CyberChallenge.IT si svolgeranno secondo i formati classici:

- **jeopardy** (CTF locale e nazionale): l'obiettivo è, in questo caso, risolvere il maggior numero di sfide, consistenti, ad esempio, nell'identificare le vulnerabilità di un programma o di ottenere accesso a un sistema; ogni sfida risolta equivale alla conquista di una "flag" e fornisce un certo numero di punti;
- **attack-defense** (solo CTF nazionale): ogni giocatore (o team di giocatori) contribuisce con un server a un'arena comune. L'obiettivo è conquistare flag sui server altrui (attack) e impedire che altri conquistino le flag sul proprio server (defense).

Le gare CyberChallenge.IT verteranno sui temi considerati in varie CTF internazionali, fra cui:



Recruitment fair

Secondo un formato comune in questo tipo di iniziative, sono organizzati, sia a livello locale sia a livello nazionale, dei *recruitment fair*, vale a dire dei momenti di incontro tra i partecipanti alla challenge e le aziende che hanno sponsorizzato l'evento e che avranno così l'opportunità di illustrare le possibilità di carriera e stabilire contatti diretti con giovani di talento.

I recruitment fair si svolgeranno a valle delle cerimonie di premiazione.

Presentazioni dei concorrenti

Come avviene in altre competizioni internazionali come la European Cybersecurity Challenge, gli eventi includeranno presentazioni **in lingua inglese** dei concorrenti che illustreranno le soluzioni alle challenge proposte utilizzando un linguaggio comprensibile a un pubblico non esperto, dimostrando di essere in grado di mettere in prospettiva gli aspetti tecnici nel contesto più ampio della rivoluzione digitale dei nostri tempi.

I concorrenti saranno stati istruiti su come fare presentazioni efficaci durante le lezioni orizzontali svolte durante i corsi, parte delle quali verteranno sui "soft skill" necessari in una carriera in cybersecurity.

2.5.1 Evento CTF locale

La CTF locale sarà **individuale** nello stile **jeopardy**.

I **primi tre classificati** formeranno la squadra locale che parteciperà alla CTF nazionale.

Al riguardo, si ritiene che un modello di gara individuale permetta di valutare le qualità dei singoli ai fini del successivo reclutamento per la Squadra Nazionale di Cyberdefender.

Le gare CTF locali si svolgeranno su due giorni, simultaneamente in tutte le sedi:

- giovedì 7 giugno 2018: competizione CTF su piattaforma CINI
- venerdì 8 giugno 2018:
    - **mattina**: cerimonia di premiazione alla presenza delle istituzioni universitarie locali, della stampa e delle aziende. Oltre ai primi tre classificati alla CTF locale, verranno premiati tutti gli ammessi a CyberChallenge.IT con una targa che ne attesta l'ammissione e la partecipazione. A seguito della cerimonia di premiazione, i tre premiati faranno una breve presentazione in cui discutono le soluzioni alle CTF proposte.
    - **pomeriggio**: recruitment fair locale con gli sponsor.

Le challenge assegnate alle CTF locali saranno **identiche per tutte le sedi** e fornite dal CINI.

2.5.2 Evento CTF nazionale

La CTF nazionale sarà organizzata a *squadre* nello stile *attack/defense*. Come avviene in altre competizioni come la European Cybersecurity Challenge, le squadre verranno valutate secondo due criteri:

- numero di "flag" catturate
- chiarezza ed efficacia della presentazione delle soluzioni alle challenge risolte, valutate da una giuria (composizione da definirsi).

Ciascuna sede locale avrà diritto all'invio di una squadra di 3 membri, opportunamente selezionati durante la CTF locale.

La CTF nazionale si svolgerà su due giorni secondo il seguente **programma tentativo**:

- mercoledì 27 giugno 2018:
  - briefing squadre
  - competizione CTF su piattaforma CINI
- giovedì 28 giugno 2018:
  - mattina:
    - **presentazioni** in cui le squadre illustrano le soluzioni alle CTF svolte
    - **talk degli sponsor nazionali** e contemporaneamente valutazione delle presentazioni da parte della giuria
    - **cerimonia di premiazione** alla presenza delle istituzioni governative nazionali, del Rettore di Sapienza Università di Roma, della stampa e delle aziende
  - pomeriggio:
    - **recruitment fair** con gli sponsor nazionali aperto a tutti gli studenti ammessi a CyberChallenge.IT presso le varie sedi, che parteciperanno all'evento a proprie spese
    - **sala stampa** con i giornalisti.

I partecipanti alla CTF nazionale avranno successivamente la possibilità di essere convocati nella Squadra Nazionale di Cyberdefender italiana, allenata e gestita dal Laboratorio Nazionale di Cybersecurity del CINI.

2.6 Dopo la challenge

Condividere tre mesi di corso e l'esperienza delle gare crea una comunità di giovani appassionati desiderosi di rimanere in contatto fra loro e con gli istruttori. Piacevoli esperienze finali sono una "cyberbirra" e/o una "cyberpizza" con cui festeggiare in modo conviviale i mesi trascorsi insieme. Molti dei giovani che hanno partecipato a CyberChallenge.IT si sono resi disponibili a collaborare negli anni successivi per le sessioni di addestramento e per portare la propria testimonianza alle nuove leve.

Un secondo aspetto dopo la CTF nazionale sarà la formazione e l'allenamento della *Squadra Nazionale di Cybersecurity* (Paragrafo 3).

3. Squadra Nazionale Italiana Cyberdefender

Il CINI ha siglato un accordo con il Ministero per lo Sviluppo Economico (MISE) per formare una Squadra Nazionale Italiana Cyberdefender che rappresenti l'Italia nelle competizioni internazionali.

La nazionale italiana 2017, dal nome evocativo "8bITs - get a byte of Italy", è composta da 3 giovani di categoria junior (14-20 anni) e 5 giovani di categoria senior (21-25 anni). Il team include i vincitori dell'edizione 2017 di CyberChallenge.IT e membri senior delle squadre di cyberdefender dell'Università Ca' Foscari di Venezia e del Politecnico di Milano con grande esperienza nelle competizioni internazionali dedicate alla sicurezza informatica.

I giovani atleti sono Pietro Borrello, Qian Matteo Chen, Andrea Fioraldi, Dario Petrillo e Simone Primarosa (CyberChallenge.IT 2017), Marco Festa (team towerofhanoi del Politecnico di Milano) e Francesco Benvenuto e Lorenzo Veronese (team c00kies@venice della Ca' Foscari). La squadra nazionale è allenata dal coach Marco Squarcina (Ca' Foscari), da Francesco Palmarini (Ca' Foscari) e da Emilio Coppa (Sapienza).

La squadra azzurra si è allenata dal 9 al 12 ottobre presso la Scuola IMT Alti Studi Lucca.

3.1 Successo italiano all'European Cybersecurity Challenge 2017

Il 1 novembre 2017 l'Italia ha partecipato con la propria squadra per la prima volta all'European Cybersecurity Challenge (ECSC), la principale competizione europea per cyber-defender, ottenendo la **medaglia di bronzo** (a pari merito con UK) su 15 nazioni dopo Spagna e Romania.

All'evento, promosso dall'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione (ENISA) e dedicato a giovani tra i 14 e i 25 anni, hanno partecipato le squadre nazionali di Austria, Cipro, Repubblica Ceca, Danimarca, Estonia, Germania, Grecia, Irlanda, Italia, Liechtenstein, Norvegia, Romania, Spagna, Svizzera e Regno Unito.

L'edizione di quest'anno è durata dieci ore e ha incluso temi particolarmente impegnativi fra cui l'identificazione di vulnerabilità in dispositivi hardware come lettori di smart card e serrature elettroniche.

Ogni team è stato valutato non solo per il talento tecnico, ma anche per la capacità di collocare le problematiche trattate nel contesto della rivoluzione digitale dei nostri tempi, presentando alla giuria le soluzioni alle sfide proposte con un intervento breve ma di ampio respiro accessibile anche a non esperti.

4. Gestione del progetto

Il Leader del Progetto è il Prof. Camil Demetrescu (Sapienza Università di Roma). La responsabilità della pianificazione a medio-lungo termine e del successo del Progetto è affidata a uno Steering Committee di cui fanno parte:

- Prof. Roberto Baldoni, Direttore del LNCS CINI, Sapienza Università di Roma
- Prof. Camil Demetrescu, Project Leader, Sapienza Università di Roma
- Dott.ssa Angela Miola, Direttore Esecutivo del CINI
- Prof. Paolo Prinetto, Presidente del CINI, Politecnico di Torino

5. Contatti

Per maggiori informazioni contattare la segreteria CyberChallenge.IT all'indirizzo cyberchallenge@consorzio-cini.it.