Progetto CyberChallenge.IT 2020 – Presentazione

Indice

CINI Cybersecurity National Lab
c/o DIAG - Sapienza Università di Roma
Via Ariosto, 25 – 00185 Roma RM

https://cybersecnatlab.it

Contatti:
segreteria.cybersecurity@consorzio-cini.it
http://www.cyberchallenge.it/

1 Introduzione

Questo documento ha l'obiettivo di presentare il progetto CyberChallenge.IT, con particolare riferimento ai suoi aspetti generali e ai dettagli specifici dell'edizione 2020.

Vengono dapprima illustrati gli obiettivi del progetto e le diverse fasi del percorso formativo (sez. 2). La sez. 3 è dedicata alla realtà della *Squadra Nazionale di Cyberdefender*, chiamata a rappresentare il Paese nelle principali competizioni internazionali, con una breve presentazione delle principali competizioni internazionali nelle quali sarà coinvolta.

2 Il progetto

2.1 Presentazione

2.1.1 Missione

CyberChallenge.IT è un programma di formazione per i giovani talenti che punta a ridurre significativamente l'odierna carenza della forza lavoro in ambito informatico, ponendosi come la principale iniziativa italiana per identificare, attrarre, reclutare e collocare la prossima generazione di professionisti della sicurezza informatica. L'obiettivo per l'edizione 2020 è di coinvolgere almeno 4.000 tra i migliori studenti in Italia e di incoraggiarli a riempire i ranghi dei futuri professionisti della cybersecurity, mettendo così a disposizione del sistema paese le loro capacità.

2.1.2 A chi è rivolto

I candidati sono giovani fra 16 e 23 anni che vivono in Italia.

2.1.3 Obiettivi

Il progetto mira a creare e far crescere la comunità dei cyberdefender investendo sui giovani. In particolare punta a:

- stimolare l'interesse verso le materie tecnico scientifiche e, in particolare, verso l'informatica;
- far conoscere le opportunità professionali offerte dai percorsi formativi sulla sicurezza informatica;
- mettere i giovani in contatto diretto con realtà aziendali, anche grazie alle sfide che saranno chiamati ad affrontare;
- identificare i giovani talenti cyber e contribuire al loro orientamento e alla loro formazione professionale.

2.1.4 Metodologia e contenuti formativi

Il programma affianca un'attività formativa tradizionale a un approccio orientato alla *gamification* che si traduce nella partecipazione a competizioni in arene virtuali che simulano scenari di reti e ambienti lavorativi reali. Il modello proposto è unico nel suo genere nel panorama internazionale; esso infatti prevede non solo il ricorso al *gaming* come strumento di attrazione per i giovani, ma anche un significativo percorso formativo multidisciplinare. Tale percorso è incentrato sull'introduzione tecnica, scientifica ed etica alle tematiche connesse alla sicurezza informatica, alternando lezioni teoriche ed esercizi su vari argomenti quali crittografia, analisi di malware e sicurezza web.

2.1.5 Modalità di partecipazione

Gli studenti vengono selezionati, a seguito di informazione capillare nelle scuole superiori e nelle università, tramite due test. Il primo viene svolto on-line da remoto e serve per una prima selezione; il secondo viene invece svolto in presenza presso le diverse università aderenti al progetto e serve per la formazione delle squadre.

L'edizione 2020, come le precedenti, offrirà agli studenti selezionati corsi di addestramento presso le sedi universitarie partecipanti e culminerà nel *terzo campionato italiano Capture-The-Flag (CTF) in cybersecurity* che permetterà di identificare la *Squadra Nazionale di Cyberdefender* che parteciperà alla European Cyber Security Challenge (ECSC)[1]. L'edizione 2020 mirerà anche alla ricerca e alla selezione di un numero maggiore di talenti femminili, sperimentando forme innovative per il loro coinvolgimento e punterà a un maggiore coinvolgimento degli studenti delle scuole superiori, anche attraverso l'attivazione di "*Percorsi per le competenze trasversali e per l'orientamento*"[2].

2.1.6 Impatto

Il progetto CyberChallenge.IT si pone come una iniziativa a servizio degli stakeholder locali e nazionali mirata a:

- Valorizzare i talenti a beneficio del sistema formativo e degli stakeholder del territorio (pubbliche amministrazioni, aziende, agenzie governative, etc.);
- Fornire una immediata risposta all'urgenza del paese di avere a disposizione nuove figure professionali legate al settore della sicurezza informatica;
- Garantire ai giovani selezionati e alle università, agli enti e alle aziende sostenitrici visibilità a livello nazionale e internazionale;
- Offrire sostegno ai giovani per l'orientamento verso carriere e programmi di placement in ambito cybersecurity, anche grazie al supporto e al coinvolgimento rappresentanti di importanti aziende italiane e internazionali;
- Promuovere lo sviluppo del progetto sia a livello locale, prevedendo espansioni sul territorio, sia internazionale, esportando la formula e la piattaforma in altri paesi.

2.2 Gli asset del progetto per il Sistema Paese

L'attuale rivoluzione tecnologica e le sue implicazioni sistemiche sono strettamente legate alla definizione del fenomeno ICT come insieme di sfide comuni che Istituzioni, Aziende, Ricerca e singoli cittadini devono necessariamente affrontare. Pertanto, se da un lato il cyberspazio diventa sempre più un'infrastruttura critica, che funge da snodo nel processo di fornitura di servizi essenziali, dall'altro esso presenta vulnerabilità derivanti dalla propria natura: un mondo di creazione umana, parallelo ma anche ormai profondamente correlato a quello naturale e basato sulla trasmissione di dati e informazioni. In questo contesto, la cybersecurity è ovunque: nell'hardware, nel software, nei sistemi di comunicazione, nei processi aziendali, nei servizi pubblici, ... La sicurezza informatica diventa quindi l'elemento essenziale di questa nuova dimensione per garantire, nel tempo, un adeguato livello di sicurezza per le nostre relazioni, le nostre imprese e le nostre democrazie.

Attualmente l'Italia sta lottando per rispondere adeguatamente ad alcune delle sfide, perché il numero di professori e ricercatori di sicurezza informatica è ancora troppo basso; le università e

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

[2] https://miur.gov.it/web/guest/-/linee-guida-dei-percorsi-per-le-competenze-trasversali-e-per-l-orientamento

gli istituti di ricerca hanno difficoltà a mettere a punto adeguati piani di insegnamento e di ricerca e le imprese hanno difficoltà ad assumere persone con le competenze adeguate. Per invertire questa tendenza, sono necessari investimenti finanziari e di idee che coinvolgano le Università, la Ricerca, la Pubblica Amministrazione e le Aziende private.

Il progetto CyberChallenge.IT vuole essere un contributo in questa direzione, essendo il suo principale obiettivo proprio quello di creare e far crescere la comunità dei cyberdefender individuando i giovani talenti da indirizzare verso una carriera nella sicurezza informatica, attirando il loro interesse attraverso sfide informatiche, simulazioni in ambienti virtuali protetti e, in generale, attraverso iniziative che permettano ai partecipanti di sperimentare possibili contesti operativi e di valutare opportunità di crescita professionale. Il *gaming* viene utilizzato come strumento di attrazione per le giovani leve, ma viene accompagnato da un significativo percorso formativo multidisciplinare; inoltre, la fase di selezione permette alle varie università italiane di presentare a tanti giovani le loro attività formative (lauree, master, lauree magistrali) collegate a problematiche di sicurezza informatica.

In questo modo, il progetto, incoraggiando più giovani a studiare discipline informatiche, farà crescere il numero di specialisti di cybersecurity che potranno contribuire a rendere più sicure le aziende operanti in Italia e le Pubbliche Amministrazioni locali. Inoltre, selezionando i migliori talenti e rendendo disponibili i loro curriculum alla Pubblica Amministrazione centrale, darà al Paese l'opportunità di attingere a un serbatoio di competenze che sono indispensabili per mettere in sicurezza il nostro Paese e la nostra democrazia.

Una ricaduta rilevante del progetto è infine costituita dalla formazione della *Squadra Nazionale Italiana Cyberdefender,* che sta rappresentando con successo l'Italia nelle competizioni internazionali più rilevanti, quali la *European Cyber Security Challenge* (ECSC), la principale competizione europea per cyberdefender promossa dalla European Union Agency for Cybersecurity (ENISA). Della Squadra Nazionale vengono chiamati a far parte i ragazzi che meglio hanno dimostrato le proprie capacità, sia a livello individuale, sia come gioco di squadra, durante le varie fasi della CyberChallenge.IT.

La partecipazione a queste competizioni europee, seppur globalmente particolarmente onerosa, rappresenta una notevole opportunità di visibilità per l'Italia, al punto che riteniamo particolarmente significativo candidarci, proprio come "sistema Paese", a ospitare e organizzare la competizione europea ECSC nella prima data possibile, vale a dire nell'autunno del 2023.

2.3 Ruolo dei principali stakeholder

Per quanto detto sopra, il progetto CyberChallenge.IT vede coinvolti molteplici attori che, sinergicamente, contribuiscono all'organizzazione, al finanziamento, alla visibilità e al successo dell'iniziativa, tra i quali vanno evidenziati:

- *Laboratorio Nazionale Cybersecurity del CINI*
- *Comparto Intelligence Nazionale*
- *Ministero della Difesa*
- *Ministero dell'Istruzione, dell'Università e della Ricerca*
- *Ministero degli Affari Esteri e della Cooperazione Internazionale*
- *Sistema Universitario Italiano*
- *Aziende private.*

In particolare, il *Laboratorio Nazionale Cybersecurity* opera da coordinatore dell'intero progetto, ne gestisce le diverse fasi, che vanno dalla promozione alla gestione quotidiana, e garantisce la qualità dei percorsi formativi. Il Laboratorio, inoltre, mantiene i contatti con le sedi universitarie

e con i diversi stakeholder che aderiscono al progetto. Il Laboratorio contribuisce anche al finanziamento, mettendo a disposizione proprio personale e proprie attrezzature.

Siccome sta emergendo sempre più che la cybersecurity e quindi la disponibilità di figure professionali in grado di garantirla sono essenziali per la Sicurezza del nostro Paese, il progetto beneficia della collaborazione con il *Comparto Intelligence Nazionale* e con il *Ministero della Difesa*. Il primo considera il progetto in linea con quanto previsto dal *Piano Nazionale per la protezione cibernetica e la sicurezza*, mentre il secondo contribuisce all'organizzazione della competizione finale nazionale, anche ospitandola presso proprie strutture.

Il *Ministero dell'Istruzione, dell'Università e della Ricerca*, che ritiene importanti tutte quelle iniziative che puntino a incoraggiare i giovani allo studio di discipline tecnico scientifico (STEM), promuove il progetto verso tutti gli istituti scolastici superiori, anche attraverso avvisi mirati, e contribuisce al supporto delle attività nell'ambito di "Percorsi per le competenze trasversali e per l'orientamento".

Il *Ministero degli Affari Esteri e della Cooperazione Internazionale,* attraverso la Direzione Generale per la Promozione del Sistema Paese e il Commissario Generale Aggiunto per Expo 2020 Dubai, ha inserito il progetto CyberChallenge.IT all'interno del programma di iniziative concernenti i temi della Cybersecurity che si svolgeranno nel corso del semestre dell'Esposizione universale *Expo 2020 Dubai*, come noto dedicata al tema "Connecting minds, creating the future" (ottobre 2020 - aprile 2021).

Ovviamente il progetto si avvale della collaborazione dei diversi attori del *Sistema Universitario Italiano*: nell'edizione 2019 sono state ben 18 le sedi universitarie che hanno aderito al progetto. Le singole università utilizzano il progetto anche come un'occasione per pubblicizzare le proprie lauree in discipline informatiche e, soprattutto, forniscono supporto allo svolgimento del percorso formativo, in termini di spazi e di personale docente coinvolto. Significativo, al riguardo, anche il ruolo dei *Centri di Competenza Regionali in Cybersecurity* che stanno ora nascendo in diverse regioni italiane come forma di collaborazione tra università e centri di ricerca per attività di ricerca e supporto alle imprese e alla pubblica amministrazione locale.

In questa fase, la carenza di esperti in sicurezza informatica sta mettendo in difficoltà tante aziende a livello internazionale e l'Italia non è un'eccezione. Per questo assistiamo con piacere alla disponibilità di varie *Aziende Private* a supportare economicamente, attraverso sponsorizzazioni e in alcuni casi anche attraverso la messa a disposizione di competenze specifiche e di rilevanti casi di studio industriali, per l'attività formativa. In cambio, le aziende possono accedere ai curriculum dei giovani selezionati per la formazione e hanno l'opportunità di incontrarli in occasione di eventi mirati, organizzati in occasione delle gare locali e di quella nazionale.

2.4 Edizioni passate

Il progetto è giunto alla quarta edizione. La Tabella 1 riporta l'evoluzione delle tre edizioni precedenti e mostra che per l'edizione 2019, dopo i due test sono stati selezionati 360 giovani tra i 3.200 inizialmente iscritti. Questi giovani hanno seguito un percorso formativo multidisciplinare, presso 18 sedi universitarie distribuite sul territorio nazionale. Alla fine di tale percorso, ha avuto luogo prima una competizione locale con sfide uguali e contemporanee in tutte le sedi, e poi una gara nazionale: il secondo campionato italiano Capture-The-Flag (CTF) in cybersecurity, organizzato a Chiavari (GE) congiuntamente dal Laboratorio Cybersecurity del CINI e dalla *Scuola Telecomunicazioni Forze Armate (STELMILIT)*, sotto il patrocinio del *Sistema di informazione per la sicurezza della Repubblica* e del *Ministero della Difesa*.

Dal 2018, CyberChallenge.IT è supportato dal Sistema di Informazione per la Sicurezza della Repubblica, Presidenza del Consiglio dei Ministri e l'edizione 2019 ha avuto anche il patrocinio del Ministero della Difesa.

Nel 2018 e nel 2019, il Nucleo di Sicurezza Cibernetica (NSC) ha affidato al Laboratorio Nazionale di Cybersecurity del CINI il compito di organizzare e gestire le attività della Nazionale Italiana di Cyberdefender e la partecipazione alle competizioni internazionali del settore.

Tabella 1 - Partecipanti alle precedenti edizioni del progetto

Anno	Sedi	Studenti coinvolti								
		Iscritti							Ammessi	
		Totale	Genere		Provenienza					
			M	F	Scuole superiori		Università			
		#	#	#	#	%	#	%	#	%
2017	1	**683**	603	80	57	8,3	626	91,7	**20**	2,9
2018	8	**1.866**	1.698	168	583	31,2	1.283	68,8	**160**	8,6
2019	18	**3.203**	2.830	373	1.341	41,9	1.862	58,1	**360**	11,2

2.5 Fasi di svolgimento

Ciascuna edizione del progetto CyberChallenge.IT prevede:

1. L'*iscrizione* (gratuita) al progetto da parte degli studenti interessati tramite il portale del progetto: www.cyberchallenge.it.
2. La possibilità di *training al test di ammissione* tramite la piattaforma che sarà utilizzata per il test; questa permette agli studenti iscritti di accedere sia agli esercizi delle edizioni precedenti sia a una simulazione dei test.
3. Un *test di ammissione* volto a selezionare studenti con eccellenti capacità logiche, di problem-solving e di programmazione; non sono richieste conoscenze pregresse su temi di cybersecurity.
   Il test di ammissione si svolge in due fasi:
   a. test on-line che, se superato, consente l'accesso al successivo, in presenza;
   b. test in presenza, svolto contemporaneamente presso tutte le sedi coinvolte, che porta a selezionare un gruppo di 20 partecipanti per ciascuna sede.
4. 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 viene svolto presso ciascuna sede in orari compatibili con le attività didattiche degli studenti (es. venerdì pomeriggio/sabato mattina).
5. Una *gara CTF locale individuale,* mirata a selezionare i migliori studenti di ciascuna sede. Presso ciascuna sede, alla gara segue una premiazione locale e una recruitment fair in cui gli studenti hanno l'opportunità di incontrare gli sponsor locali.
6. *Una gara CTF nazionale a squadre* (una squadra per ciascuna sede locale) che prevede:
   a. una *cerimonia di premiazione nazionale* presieduta da rappresentanti delle istituzioni italiane;
   b. un *incontro con le aziende*, in cui i giovani incontrano le aziende sponsor a livello nazionale.

2.6 Iscrizioni e partecipazione

Per l'edizione 2020, le iscrizioni sono aperte ai giovani nella fascia di età compresa tra i 16 e i 23 anni compiuti nel 2019, vale a dire per i nati negli anni 1996-2003; l'iscrizione è gratuita.

2.7 Cronologia delle attività per l'edizione 2020

La cronologia delle attività per l'edizione 2020 è riassunta nella Tabella 2.

Tabella 2 - Cronologia dell'edizione 2020 del progetto

Attività	Date
Adesione delle sedi	Entro il 30/11/2019
Adesione delle aziende sponsor	Entro il 30/11/2019
Iscrizioni on-line	02/12/2019 - 17/01/2020
Pre-Test on-line	22/01/2020 - 24/01/2020
Test di ammissione	17/02/2020
Percorso formativo	02/03/2020 - 30/05/2020
Gare a livello locale	08/06/2020
Cerimonie di premiazione a livello locale	09/06/2020
Challenge nazionale	09/07/2020
Cerimonia di premiazione a livello nazionale	10/07/2020

2.8 Incentivi per gli studenti partecipanti

Oltre alla visibilità mediatica e al riconoscimento pubblico delle loro abilità, i partecipanti ricevono premi di vario tipo e natura, quali medaglie, attestati, dispositivi elettronici.

Nel seguito vengono presentate tre nuove iniziative mirate a offrire agli studenti partecipanti riconoscimenti a livello di carriera scolastica.

2.8.1 Progetto Valorizziamo i talenti

Sono allo studio con la *Conferenza dei Rettori delle Università italiane* (CRUI), meccanismi per far sì che le Università possano offrire facilitazioni di vario tipo per le iscrizioni/immatricolazioni mirate inizialmente a coinvolgere il maggior numero di giovani e, successivamente, a valorizzare i "talenti" identificati attraverso il progetto, offrendo loro riconoscimenti e opportunità, grazie alla collaborazione tra il Laboratorio Nazionale di CyberSecurity del CINI, la CRUI e le Università italiane.

2.8.2 Riconoscimenti di Crediti Formativi Universitari

Il Laboratorio Nazionale di CyberSecurity del CINI raccomanda alle università aderenti al progetto CyberChallenge.IT di voler riconoscere dei CFU (Crediti Formativi Universitari) agli studenti che hanno partecipato al progetto. Visto l'impegno complessivamente richiesto a ciascun partecipante, si ritiene adeguato il riconoscimento di **6 CFU**, nelle modalità ritenute localmente più idonee.

2.8.3 Percorsi per le competenze trasversali e per l'orientamento

Alla luce dei positivi risultati ottenuti nelle sperimentazioni fatte in alcune sedi nelle scorse edizioni, si raccomanda vivamente alle Università e alle Scuole Superiori partecipanti di avviare dei *Percorsi per le competenze trasversali e per l'orientamento*.

2.9 Incentivi per le Scuole Superiori partecipanti

Alle Scuole Superiori interessate ad aderire al progetto viene proposto un *programma di federazione* che permetterà ai loro docenti l'accesso a materiale didattico addizionale finalizzato a supportarli nelle attività di addestramento dei loro studenti nella preparazione ai test di ammissione a CyberChallenge.IT.

Alle scuole aderenti sarà data adeguata visibilità sul sito web del progetto[3] e sarà fortemente raccomandato l'avvio di *Percorsi per le competenze trasversali e per l'orientamento*.

Nel corso dell'anno sarà avviato un corso pilota sperimentale su tematiche di cybersecurity mirato alla formazione dei docenti delle scuole aderenti.

3 Squadra Nazionale Italiana di Cyberdefender

Il Laboratorio Nazionale Cybersecurity ha ricevuto mandato dal Nucleo per la Sicurezza Cibernetica della Repubblica Italiana di formare una *Squadra Nazionale Italiana Cyberdefender* che rappresenti l'Italia nelle competizioni internazionali.

Della Nazionale, che ha preso il nome di *TeamItaly*, vengono chiamati a far parte i ragazzi che meglio hanno dimostrato le proprie capacità, sia a livello individuale, sia come gioco di squadra, durante le varie fasi della CyberChallenge.IT.

Ad allenare la squadra è stato chiamato, nel 2019, il Dr. Mario POLINO (Politecnico di Milano).

La partecipazione a competizioni internazionali, seppur globalmente particolarmente onerosa, rappresenta una notevole opportunità di visibilità per il Paese.

3.1 European Cyber Security Challenge (ECSC)

Per mitigare la mancanza di esperti nel settore della sicurezza informatica, molti paesi hanno lanciato competizioni volte a scoprire i giovani talenti e incoraggiare le nuove generazioni a perseguire una carriera in cybersecurity.

[3] https://www.cyberchallenge.it

A livello italiano l'iniziativa più significativa è il progetto CyberChallenge.IT, del Laboratorio Nazionale Cybersecurity del CINI, che offre un percorso di addestramento gratuito e la possibilità di entrare a far parte della nazionale Italiana di cyberdefender.

A livello europeo, ENISA (*European Union Agency for Cybersecurity*) fa da volano e, facendo tesoro delle esperienze delle singole nazioni, organizza ogni anno la *European Cyber Security Challenge* (ECSC) con lo scopo di favorire lo scambio di conoscenza e talenti su tutta Europa. La competizione è aperta a tutti i paesi europei. Ogni nazione che si iscrive all'evento partecipa con una squadra composta da 10 giocatori di un'età compresa tra i 14 e i 25 anni.

L'Italia ha partecipato per la prima volta a ECSC nel 2017 conquistando il terzo posto (a pari merito con il Regno Unito). Nel 2018 ha ottenuto la sesta posizione.

Nel 2019 la competizione, giunta ormai alla sua sesta edizione, è stata ospitata dalla Romania dall'8 al 12 Ottobre presso il Palazzo del Parlamento a Bucarest e ha visto la partecipazione di 20 paesi. Il comitato organizzativo era composto, in aggiunta all'ENISA, dal *National Cyberint Center* (Romanian Intelligence Service, SRI), dal *CERT-RO* (Romanian National Computer Security Incident Response Team, coordinated by the Ministry of Communications and Information Society) e dal *National Association for Information Systems Security* (ANSSI). In questa edizione la Nazionale Italiana ha conquistato il podio, guadagnandosi il secondo posto, preceduta solo dalla Squadra Rumena.

La prossima edizione della competizione si svolgerà a Vienna dal 4 al 6 novembre 2020.

In preparazione alla partecipazione a ogni edizione della ECSC, la squadra è convocata per una settimana di "ritiro" presso l'IMT di Lucca.

3.2 Partecipazione a *Expo 2020 Dubai*

Nell'ambito della *Cyberweek* organizzata dal *Ministero degli Affari Esteri e della Cooperazione Internazionale* nell'ambito dell'Esposizione universale *Expo 2020 Dubai*, oltre alla presentazione del progetto CyberChallenge.IT in una prestigiosa vetrina internazionale, il Laboratorio Nazionale Cybersecurity del CINI è chiamato a organizzare una competizione nella quale la Squadra Nazionale Italiana di Cyberdefender incontrerà altre squadre nazionali parigrado.