

ITASEC21, LA PRINCIPALE CONFERENZA NAZIONALE SULLA SICUREZZA NAZIONALE, RADDOPPIA: 1800 ISCRITTI E CENTINAIA DI VISUALIZZAZIONI IN STREAMING

www.itasec.it

Comunicato stampa - Roma, 12 aprile 2021

Oltre **1800 partecipanti**, 52 sessioni e 4 distinte track hanno confermato l'importanza di Itasec, la principale conferenza italiana di sicurezza informatica, che si è svolta per la prima volta quest'anno interamente online a causa delle restrizioni sanitarie. La pandemia non ha scalfito lo spirito dell'evento, giunto alla quinta edizione, che ha raccolto - virtualmente - ospiti e contenuti di elevato valore scientifico, tecnico, socio-politico, favorendo la **condivisione di conoscenze** ed esperienze nel campo della sicurezza informatica, sempre più centrale nella quotidianità di tutti.

Dopo la fortunata edizione del 2020, che ha portato ad Ancona più di **ottocento persone**, Itasec21 raddoppia il numero degli spettatori registrati e a questi aggiunge le centinaia di persone che hanno seguito in diretta streaming **decine di ore di conferenze e dibattiti**, con una presenza complessiva di oltre tremila spettatori. Sui quattro palchi, *workshop, stakeholder space, scientific & technical sessions, vendor sessions* si sono tenuti rispettivamente 9, 17, 14 e 12 incontri, che hanno assicurato una presenza media di **80 persone a panel**.

“Un successo che ci ripaga di ogni sforzo e che dimostra quanto il tema della sicurezza informatica sia sempre più centrale e rilevante per tecnici, accademici, aziende e anche solo persone interessate alla materia, dalle quali abbiamo ricevuto ringraziamenti e feedback positivi” - ha dichiarato Paolo Prinetto, direttore del Laboratorio Nazionale di Cybersecurity del CINI -. *Tra gli argomenti che consuetudinariamente trovano spazio tra le sale di Itasec21, sempre concentrati sul futuro e l'innovazione, quest'anno si è fatta strada anche una ricerca di risposte alla sicurezza nella nostra quotidianità, in conseguenza a un anno particolarmente provante anche dal punto di vista del digitale. Crediamo di aver suggerito e ispirato i nostri ospiti e il pubblico e siamo convinti che sempre più persone si lasceranno coinvolgere dal fascino della rete e della sua protezione. Naturalmente nella speranza di poter riprendere questo discorso, stavolta in presenza, a Itasec22”*.

I lavori si sono aperti con l'introduzione a cura di Paolo Prinetto, direttore del **Laboratorio Nazionale di Cybersecurity del CINI** (Consorzio Interuniversitario Nazionale per l'Informatica), e dei co-chair di Itasec21, Michele Colajanni, Alessandro Armando e Rocco De Nicola. A seguire, l'atteso [keynote speech](#) dell'ospite d'onore di questa giornata, il Direttore generale di DG CONNECT (Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie) presso la Commissione Europea, **Roberto Viola**. Già Chairman dello European Radio Spectrum Policy group (RSPG) e Segretario generale di AGCOM, Viola ha presentato una panoramica degli sforzi compiuti a livello europeo nel sostenere la crescita del settore, con particolare riguardo al ruolo politico e regolatorio che è indispensabile per accrescere la resilienza delle infrastrutture

<https://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it

comunitarie. Come ricordato da Viola, lo sviluppo digitale è un bene indispensabile nel rafforzamento di un **sistema europeo solido**, che richiede un forte sostegno sul piano politico, su quello regolatorio e su quello proprio della cybersecurity, che protegge gli interessi e gli investimenti dell'intera Comunità Europea.

L'ultimo dei preziosi interventi della rassegna ha visto la partecipazione del prof. **Roberto Baldoni**, Vicedirettore Generale del Dipartimento delle informazioni per la sicurezza (Dis), che ha offerto una panoramica delle misure tecniche e legislative adottate in questi anni per rafforzare la tenuta del "Sistema Paese". Proprio a Itasec, a Pisa nel 2019, Baldoni aveva presentato i primi passi di un percorso che è andato compendosi nel tempo e che, dopo due anni, registra l'avvio concreto del **Perimetro di sicurezza nazionale cibernetica**, che, con i relativi decreti attuativi, riorganizza la logica della sicurezza in Italia in favore di una migliore gestibilità delle minacce domestiche e internazionali. Baldoni ha anche elogiato le iniziative del Laboratorio Nazionale di Cybersecurity, [CyberChallenge.IT](#) e [Olicyber](#), che coinvolgendo studentesse e studenti fin dal primo anno di scuola superiore di secondo grado, garantiscono un percorso d'eccellenza unico per accedere al mondo della sicurezza informatica: "Un fiore all'occhiello che contribuisce a rendere l'Italia rilevante a livello internazionale", ha detto Baldoni.

Tra gli ospiti più prestigiosi della rassegna, in apertura del palco principale nella giornata conclusiva, anche il Procuratore Aggiunto della Direzione Nazionale Antimafia e Antiterrorismo, **Giovanni Russo**, con una presentazione sugli strumenti tecnologici che abilitano quotidianamente il contrasto al terrorismo e alle attività illecite. Ma la sicurezza e le diverse sfumature che questa può assumere sono stati il *leitmotiv* dell'evento, che ha spaziato **dal 5G fino alla protezione delle infrastrutture in orbita**, per fornire la più ampia rassegna di scenari nei quali l'industria e la ricerca si muoveranno nei prossimi anni.

Non è mancata, da questo punto di vista, neanche la filosofia in materia di sicurezza, protagonista del *keynote speech* di **Luciano Floridi**, professore di Sociologia della comunicazione all'Università di Bologna, tornato da poco in Italia dopo una lunga attività di insegnamento all'Università di Oxford, che ha trattato il problema della valutazione e della gestione del rischio nella "*hyper history*" in cui stiamo vivendo. L'analisi si è concentrata sugli aspetti pratici connessi alla conversione dei rischi in costi e sul ruolo del comparto assicurativo in questo scenario.

Prezioso e ampiamente partecipato è stato anche l'intervento di **Nunzia Ciardi**, Dirigente Superiore della Polizia di Stato e Direttrice del Servizio Polizia Postale e delle Comunicazioni, che ha reso una panoramica del modo in cui la pandemia di Covid-19 ha influito sui pericoli cibernetici in Italia, descrivendone l'evoluzione nell'ultimo anno. Un punto di vista unico, quello presentato, che aiuta a capire il modo in cui evolvono i crimini informatici e quali sono le misure migliori per prevenirli.

Nella stessa giornata, ha goduto di ampio successo il keynote della Scientific track tenuto da **Lujo Bauer**, docente di Scienze informatiche e Computer engineering della Carnegie Mellon University

<https://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it

(Pittsburgh, Pennsylvania), sull'impatto degli attacchi agli algoritmi di Machine Learning e sulle dinamiche che modificheranno nei prossimi anni il modo in cui intendiamo la protezione digitale e le stesse modalità di attacco.

Infine, [l'Innovation Hub \(IH\)](#) del CINI ha organizzato un incontro sul tema della commercializzazione della ricerca e sulle iniziative di supporto, promozione e accesso al finanziamento per le start up, spin off e PMI interessate ad accreditarsi nell'ecosistema cybersecurity nazionale ed europeo. Le due sessioni, coordinate da Luigi Martino e Giulio Busulini, si sono focalizzate sull'accesso all'industria, analizzando fabbisogno e desiderata tecnologici, e agli aspetti più finanziari dell'innovazione cyber, in cui sono stati coinvolti alcuni stakeholder nazionali interessati a sostenere progetti e aziende innovative cyber.

Sono ancora di più gli eventi, introdotti dai moderatori **Alessia Valentini** (Cybersecurity 360), **Sonia Montegiove** (Il Messaggero) e **Luca Zorloni** (Wired), che hanno impreziosito le giornate di Itasec. Dagli strumenti per la tutela della **pubblica sicurezza** fino a [CyberReadiness.IT](#), progetto del Laboratorio Nazionale di Cybersecurity, che mira a fornire metodologie e strumenti utili a misurare l'impatto del fattore umano nella valutazione dei rischi informatici di un'organizzazione.

Ma Itasec21 è prima di tutto un palcoscenico per il futuro: ciò che rappresenta la presentazione del [TeamItaly](#), la squadra nazionale italiana di hacker etici. Alla presenza del capitano, **Andrea Biondo**, e dell'allenatore **Mario Polino** (che ha anche offerto una presentazione sulla sicurezza degli impianti industriali), gli spettatori di Itasec hanno avuto una panoramica dei progressi fatti, nonostante la pandemia, nel perfezionare le tecniche di attacco e difesa degli atleti del Team. Il TeamItaly, **classificato secondo** alla European Cybersecurity challenge, costituisce un *unicum* a livello europeo, con una squadra attiva tutto l'anno, che ricorre a ritiri e corsi avanzati di formazione per allenarsi e rafforzare il senso di "gruppo", anche in remoto in caso di pandemia.

Una sfida, quella raccolta da TeamItaly, CyberChallenge.IT e le olimpiadi di sicurezza informatica, Olicyber, che non può prescindere da un'attenzione particolare verso l'inclusività e l'abbattimento delle **barriere di genere** nel settore, tema e missione del Laboratorio Nazionale di Cybersecurity e priorità del suo working group dedicato, **CyberEquality**, che ha presentato un panel sull'argomento. Alla guida di questa giusta e sentita battaglia - quella per **la parità delle condizioni di accesso** alle materie Stem - la professoressa **Dajana Cassioli**, docente di Ingegneria delle telecomunicazioni all'Università dell'Aquila, che con gli altri partecipanti ha promosso una riflessione sulle ragioni che maggiormente potrebbero disincentivare le donne a intraprendere una strada professionale nel settore dell'informatica e della sicurezza.

Itasec21 è cresciuta anche nella **comunicazione**, strumento fondamentale per ampliare la conoscenza nell'ambito della sicurezza informatica e per stimolare in generale il più ampio interesse nei confronti delle materie scientifiche, a beneficio degli esperti e **del pubblico tutto**. Così il convegno ha visto l'aumento complessivo dei comunicati stampa e la realizzazione di una speciale newsletter serale, **Triplesec**, che ha raccontato le giornate di convegno sostituendo

<https://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it

temporaneamente il rituale ritrovo serale con i giornalisti in ora di aperitivo. A questo si aggiunge il corso rivolto [direttamente ai giornalisti](#), valevole per i crediti professionali, organizzato in collaborazione con l'**Ordine dei giornalisti dell'Umbria**, Wired e il Centro Hermes per la trasparenza e i diritti umani digitali. L'iniziativa ha permesso di analizzare i metodi di comunicazione dei data breach e il modo più corretto di affrontarli sia dal punto di vista del cronista sia da quello dell'ufficio stampa delle aziende che eventualmente siano cadute vittima di un attacco informatico. Più concretamente, l'incontro ha anche fornito elementi utili per migliorare la protezione delle fonti e delle telecomunicazioni. L'intera iniziativa è stata accompagnata dal reporting costante dei media partner di Itasec, **La Stampa**, **Wired**, **Report Difesa** e **Cybersecurity Italia**, a conferma del sempre crescente impegno da parte della stampa sulle materie della sicurezza informatica.

A dimostrazione della crescente rilevanza di Itasec contribuisce anche un aumento della quantità di aziende sponsor, necessarie alla buona riuscita del convegno e fondamentali nell'offrire il punto di vista di chi lavora ogni giorno nel campo della sicurezza informatica, rispondendo alle esigenze di istituzioni e aziende. Questa l'opportunità offerta dagli sponsor Platinum (Accenture, aizoOn, Blu5 group, Bv Tech, Cisco, Exabeam, Exprivia, Leonardo, Microsoft Italia e Minsait), che, insieme agli sponsor Gold e Silver (7Layers, Huawei e Tiesse come Gold, Cybertech e Hermes bay come Silver) hanno sostenuto l'iniziativa.

Maggiori informazioni sono disponibili all'indirizzo

www.itasec.it

Che Cos'è il Laboratorio Nazionale di Cybersecurity - CINI

Il Laboratorio Nazionale di Cybersecurity del CINI coordina attività di ricerca e formazione sui temi della sicurezza informatica a livello nazionale e internazionale per aiutare il "sistema paese" a essere più resiliente alla minaccia cibernetica. 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://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it