

Per la prima volta online, Itasec21 reinventa anche il "terzo tempo", tradizionale chiusura delle giornate di convegno per i giornalisti interessati alla cybersecurity. Per loro nasce TripleSec, il riassunto della giornata di Itasec, da gustare con calma e con un aperitivo.

ITASEC21: RESOCONTO DEL SECONDO GIORNO DI CONVEGNO, DALLE ESPERIENZE DELLA POLIZIA POSTALE ALLA CYBER DIPLOMACY E ALLA POLITICA EUROPEA

www.itasec.it

[127.0.0.1](#), 12 marzo 2021

È stata indimenticabile la seconda giornata di Itasec21, che ha visto l'inaugurazione ufficiale del palco centrale dell'evento: lo *stakeholder space*. Centinaia di persone (ci basiamo su una stima non definitiva) si sono collegate in remoto per seguire le decine di iniziative che si sono svolte in parallelo e che hanno soddisfatto i gusti di tutto il pubblico, dalla **sicurezza informatica in orbita** ai progetti innovativi messi in campo dall'Unione Europea per costituire **un fronte comune** a beneficio della protezione dei Paesi membri.

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 comunitarie. Come ricordato da Viola, lo sviluppo digitale è un bene indispensabile nel rafforzamento di un

<https://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it

sistema europeo solido, che richiede un forte sostegno sul piano politico, su quello regolatorio e su quello proprio della cyber security, che protegge gli interessi e gli investimenti dell'intera Comunità Europea.

Sulla scia di questa tematica si ricongiunge l'incontro successivo, nel quale eccellenti ospiti hanno rappresentato le peculiarità della sempre più rilevante [diplomazia digitale](#), destinata ad avere un ruolo centrale nei rapporti politici tra Stati e comunità. Tra questi anche **Laura Carpini**, capo Unità per le politiche e la sicurezza dello spazio cibernetico del Ministero degli Esteri e **Christopher Painter**, coordinatore della sicurezza informatica al dipartimento di Stato sotto le amministrazioni Trump e Obama e fondatore del Global forum on cyber expertise.

Nella mattinata [è intervenuta](#) anche **Nunzia Ciardi**, Dirigente Superiore della Polizia di Stato e Direttrice del Servizio Polizia Postale e delle Comunicazioni, per un *keynote speech* nel quale ha descritto il 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.

È stato come essere a casa, per i membri del Laboratorio e i frequentatori abituali di Itasec, quando è stato il momento dei rappresentanti del [TeamItaly](#), la squadra nazionale italiana di hacker etici. Alla presenza del capitano, **Andrea Biondo**, e dell'allenatore **Mario Polino**, 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.

Parallelamente allo spazio *stakeholder*, ha goduto di un ampio successo il [keynote](#) della *Scientific track* tenuto da **Lujo Bauer**, docente di Scienze informatiche e Computer engineering della Carnegie Mellon University (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.

Le decine di ore di sessioni che si sono svolte parallelamente nella giornata di oggi hanno visto anche, tra gli altri, i rappresentanti di ECSO e dei quattro progetti pilota Concordia, Echo, Sparta e CyberSec4Europe, vincitori della call sulla sicurezza informatica di Horizon 2020, e i rappresentanti di iniziative di successo nel campo della sicurezza informatica provenienti da Emirati Arabi Uniti, Israele, Regno Unito e Italia. Ancora: un'intera track - le *vendor session* - ha ospitato contributi che hanno attirato l'attenzione del pubblico e degli esperti, come l'intervento di Giorgia Somma (Business development manager di Blu5) dal

<https://twitter.com/CyberSecNatLab>

Raffaele Angius

Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity

+39 320 0869746

comunicazione.cybersecurity@consorzio-cini.it

titolo “Why rely on dinosaur-age solutions for your network security and reliability” e quello di Germano Matteuzzi (Leonardo) su “Innovative solutions for a secure digital transition in Italy and Europe”. A questi si aggiungono le esperienze e testimonianze rese dai *visioneers*, rappresentanti delle [aziende sponsor di Itasec](#), che sul palco *Stakeholder* hanno avuto l’opportunità di descrivere direzioni e tendenze del futuro nel settore della sicurezza informatica, trovando modo di non trascurare l’importanza di parole come “inclusività” e “rispetto”, proprie di Itasec e condivise da tutta l’organizzazione.

Riflessione zen della serata

È diventato fondamentale abbassare le barriere culturali all’ingresso del settore della sicurezza informatica, così da renderla più inclusiva. Ci sono tantissime donne con livello tecnico pari o superiore alla media e tra noi (hacker etici, ndr) è comune confrontarci sulle nostre conoscenze. Purtroppo non sono molte ed esiste ancora una percezione che la sicurezza informatica sia una cosa da maschi, ma speriamo che programmi come CyberChallenge.IT e Olicyber possano incoraggiare sempre più ragazze a partecipare e ad avvicinarsi a questo mondo”

Andrea Biondo, capitano della nazionale italiana di hacker etici TeamItaly

Alcuni video per rallegrare la serata:

[Stakeholder space - 8 aprile 2020, pomeriggio](#)

[Giornalisti e Cybersecurity - Dalla protezione delle fonti alla comunicazione di un data breach](#)

Maggiori informazioni e il programma completo, che sarà pubblicato in questi giorni, 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