ITASEC19

ATTACCHI CIBERNETICI, SOCIAL NETWORK, HACKER ETICI E GDPR: CHI C'È E DI COSA SI PARLA A ITASEC 2019

www.itasec.it

Comunicato stampa - Roma, 29 gennaio 2019

Come reagiscono le aziende a un attacco informatico? È vero che i social network sono pericolosi? La GDPR è un'opportunità oppure no per le aziende? Esistono gli hacker buoni? **ITASEC19**, la conferenza nazionale sulla cybersecurity che si terrà a **Pisa 12 al 15 febbraio,** proverà a rispondere anche a queste domande.

L'evento, organizzato dal **Laboratorio Nazionale di Cybersecurity del CINI presso il CNR pisano,** prevede sia la presentazione di studi scientifici ed accademici sulle applicazioni di cybersecurity – dalla biometria ai computer quantistici - che una serie di incontri e riflessioni sull'uso sociale delle tecnologie. Al filone principale, **dedicato alla scienza e tecnologia della sicurezza informatica**, si affiancano infatti **workshop, tutorial, mostre e giochi di ruolo** per riflettere con linguaggi innovativi sulle sfide più complesse poste dalla cybersecurity al nostro paese.

È il caso della **gestione degli attacchi informatici** che potrebbero colpire la distribuzione della corrente elettrica. Per far comprendere la drammaticità di un evento del genere un gruppo di "attori" appartenenti al mondo delle imprese porterà in scena la **simulazione di un attacco cibernetico.** Rivolto soprattutto ai manager e ai decision maker, la simulazione della crisi aziendale viene sviluppata come un **role play game** che si svolge in diverse fasi con l'obbiettivo di proiettare lo spettatore al centro della scena subito dopo la diffusione della notizia di una interruzione dolosa della fornitura energetica. Il "game" rappresenta tutti i principali ruoli aziendali coinvolti in un caso reale - CEO, Business Director, Risk Manager, il capo del SOC, il DPO, avvocati e comunicatori - per ridurre il danno. Narrato da **Luisa Franchina** e **Corrado Giustozzi**, gli attori del gioco di ruolo provengono da realtà aziendali come Hermes Bay, Prisma, Cy4gate e Alfagroup.

A proposito di linguaggi innovativi, anche la **Polizia di Stato**, l'ITU e il Global CyberSecurity Center partecipano all'evento con una mostra itinerante pensata per i più giovani, fatta di pannelli, pillole video e giochi a quiz. La mostra, ***Dai geroglifici a Facebook*** illustra la "storia millenaria" dei mezzi usati per esaltare o distruggere la reputazione degli individui attraverso la manipolazione delle informazioni che li riguardano. Durante le visite organizzate con la Polizia Postale, verranno dati consigli e suggerimenti sull'utilizzo corretto di Internet e dei servizi digitali. La visita termina con il CyberSecQuiz. Il progetto è realizzato da **Swiss Webacademy** e **Poste Italiane**.

L'evento pisano sarà anche **l'occasione per conoscere la nazionale italiana degli "hacker buoni", la squadra italiana dei cyberdefender,** scelti attraverso CyberchallengeIT, la prima selezione

competitiva di giovani talenti informatici giunta quest'anno alla terza edizione con il coordinamento del prof. **Camil Demetrescu**.

Sul tema "caldo" della nuova **Direttiva europea per la protezione dei dati, la GDPR**, un esperto del settore come l'avvocato **Carlo Blengino** darà i suoi consigli ai presenti su come gestire al meglio la norma in rapporto alle attività amministrative.

In apertura della conferenza la ministra della Difesa, **Elisabetta Trenta**, farà il punto dello stato dell'arte delle politiche di cybersecurity a livello nazionale insieme al prof. **Roberto Baldoni**, vicedirettore generale del Dipartimento Informazioni per la sicurezza, DIS.

Molte le istituzioni presenti con rappresentanti del Ministero degli Affari Esteri, l'ambasciatore **Francesco Maria Talò**; del Ministero dello Sviluppo Economico, il direttore dell'Iscom **Rita Forsi**; del Ministero dell'Università e della Ricerca Scientifica con il presidente del CNR **Massimo Inguscio**.

Tra le imprese che hanno sponsorizzato la conferenza e che partecipano con i loro speaker figurano alcune delle realtà bancarie e industriali più importanti del paese: Cisco, Cybaze, ENI, IBM, Leonardo, Monte dei Paschi di Siena, PWC e Telsy.

La chiusura della conferenza è affidata al sottosegretario alla Difesa, **on. Angelo Tofalo** e al presidente del CINI, prof. **Paolo Prinetto.**

L'ultima data utile per iscriversi a partecipare con la quota ridotta è il 31 gennaio 2019.

Che cos'è il Laboratorio Nazionale di Cybersecurity

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 ad 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://www.consorzio-cini.it

Report: il Libro bianco

A questo link è possibile scaricare il Libro Bianco sulla cybersecurity: "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici"

https://twitter.com/CyberSecNatLab

prof. Arturo Di Corinto
Direttore della comunicazione
Laboratorio nazionale di cybersecurity
T (+39) 335 6785259
comunicazione.cybersecurity@consorzio-cini.it