Vent'anni di Forum ICT Security

Author : Redazione

Date : 28 Ottobre 2019

La ventesima edizione del Forum ICT Security, svoltasi lo scorso 16 ottobre a Roma presso l'Auditorium della Tecnica, si chiude con un **grande successo** di numeri e di contenuti: oltre 1100 partecipanti e molteplici sinergie che hanno avuto occasione di attivarsi, prospettando interessanti e proficue collaborazioni future.

Innumerevoli gli **spunti** sollevati rispetto alle più attuali sfide dell'universo cybersecurity: temi di apertura dei lavori sono state la protezione delle infrastrutture critiche - oggetto della Tavola Rotonda moderata dalla Presidente AIIC Luisa Franchina - e una digitalizzazione che "determina un potenziale in termini di miglioramento delle efficienze ma anche un aumento della superficie di attacco, rendendo la sicurezza informatica tema centrale" (Alessandro Menna, Capgemini).

Come re-agire, allora? Necessariamente su più fronti, tra cui "la battaglia per rafforzare piccole e medie imprese, i cui investimenti in difesa Cyber sono ancora irrisori, secondo il principio *Secure us to secure me*" (Marco Tulliani, Gruppo BNP Paribas), come anche la promozione di *awareness* e formazione al fine di fronteggiare la "mancanza di figure professionali dotate di *skills* adeguate, in particolare in Italia" (Fabio Sammartino, Kaspersky Lab Italia) per prevenire potenziali, gravi ricadute in comparti strategici come quello sanitario, dove "lo stato dell'arte Cyber è ancora primitivo" (Francesco Gabbrielli, Istituto Superiore di Sanità).

Gli interventi in programma hanno poi declinato gli **scenari di rischio** emersi nel contesto di profondo cambiamento dettato dall'entrata in scena dei robot industriali - "percepiti come oggetti semplici, ma vettori di rischi insospettabili ad occhi inesperti" (Davide Quarta, EURECOM) nonché dal dilagare dell'*Internet of Things* e dall'implementazione delle **reti 5G** (che, secondo Tommaso Pecorella dell'Università di Firenze, "può rappresentare mezzo sicuro e opportunità di crescita... ma attenzione alla *ownership*!")

Altri **focus tematici** hanno riguardato il moderno comparto *Automotive,* dove gli enormi cambiamenti in atto impongono "difese distribuite e basate su sistemi *cloud*, connettività permanente, gestione sicura di dati e connessioni remote" (Mirco Marchetti, UNIMORE); e il mondo dell'*E-Commerce*, che deve mantenere fermi principi di "controllo, difesa e cooperazione" per fronteggiare le crescenti mire del crimine digitale (Paolo Spagnoletti, Università LUISS Guido Carli).

Ma è stato anche ribadito (da Vincenzo Calabró, Funzionario alla Sicurezza CIS) che, nonostante tutte le possibili strategie preventive, "il fenomeno dei *Security incidents* è inevitabile: diventa dunque fondamentale l'*Incident response*" attuato secondo il "cosiddetto *OODA loop*, divisibile in due fasi, di *detection* (*Observe, Orient, Decide*) e *response* (*Act*)" seguito da "segnalazione dell'incidente a *stakeholder* e agenzie governative,

revisione dell'*IR plan*, condivisione e approfondimento della lezione appresa" concretizzando così un approccio di *security by transparency*.

Più voci, infine, hanno sottolineato come appaia prioritario incentivare **standardizzazione dei processi, consapevolezza degli utenti e contributi alle imprese** per sostenere i necessari investimenti in sicurezza informatica sul duplice livello della formazione e delle tecnologie.

Una giornata incentrata sulla consueta dialettica tra **fiducia nelle opportunità e consapevolezza dei rischi** derivanti da un'innovazione digitale vertiginosa e, spesso, poco ponderata: dialettica necessaria per affrontare in sicurezza un futuro interconnesso che è, di fatto, già presente.

Continuate a seguire i nostri **canali social**, dove nelle prossime settimane condivideremo materiali e interviste realizzate nel corso del 20° Forum ICT Security.

Alla prossima edizione!