10° Cyber Crime Conference - Comunicato Post Evento

Author : Redazione

Date : 24 Aprile 2019

La **10a edizione della Cyber Crime Conference**, svoltasi lo scorso 17 aprile nell'Auditorium della Tecnica a Roma, ha registrato una straordinaria partecipazione di pubblico con oltre 1200 visitatori, confermando la propria autorevolezza quanto a rilevanza e attualità dei contenuti trattati.

Il programma si è aperto con la **Tavola Rotonda *Cryptocurrency e Blockchain: storia, potenzialità e fattori di rischio*** - moderata dal Consulente Informatico Forense **Paolo Dal Checco** - che ha visto docenti universitari, membri delle forze dell'ordine ed esperti di settore confrontarsi sulle attuali sfide di sicurezza imposte dal mondo delle criptovalute.

Se infatti la **blockchain**, ricorda il CSO **Vincenzo Aguì**, è "un ecosistema indipendente" che - aggiunge il **Prof. Francesco Buccafurri** - "risponde, almeno in linea teorica, alla necessità di avere trust decentralizzato" è innegabile come la pseudonimizzazione concessa da questa tecnologia si presti anche a utilizzi malevoli che, soprattutto in presenza di attori *Nation-State*, possono tradursi (come rilevato dall'avv. **Fulvio Sarzana**, docente di diritto comparato delle nuove tecnologie) in "problemi geopolitici" estremamente seri. Sul fronte delle possibili soluzioni per le aziende rispetto ai rischi intrinsechi delle criptovalute, il dott. **Stefano Capaccioli** (Commercialista e Revisore legale, nonché fondatore di Coinlex) ricorda di diffidare degli imbonitori e perseguire sempre soluzioni personalizzate, in quanto "non esiste una soluzione universalmente efficace: tutto va declinato in funzione della struttura aziendale". Nella prospettiva delle risorse a disposizione delle autorità investigative, infine, il **Col. Giovanni Reccia** (Comandante del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza) evidenzia l'urgenza di superare l'attuale parcellizzazione per prevedere strutture ben definite e meccanismi di raccordo tra i diversi Corpi, al fine di mettere in campo un'adeguata strategia di contrasto alla criminalità nel cyber spazio.

La giornata ha poi visto un serrato alternarsi di contributi in cui sono stati illustrati **scenari di rischio, casi reali e strumenti operativi** per fronteggiare le minacce del crimine informatico contemporaneo.
Tra i temi trattati e le soluzioni proposte, l'importanza di framework integrati nell'ambito delle attività di prevenzione aziendale; bitcoin e attacchi *double spending*; *cryptominers* e *adaptive defense*; *Quantum computation* e *information-theoretical security*; algoritmi social e libertà di informazione; *mobile security* e necessità di costanti aggiornamenti dei sistemi operativi in ottica di sicurezza; superfici di rischio e *awareness security*.

La **multidisciplinarietà** dei profili dei relatori - Istituzioni, Aziende, Enti di ricerca - e l'incontro tra teorici e pratici della materia hanno consentito, ancora una volta, un dibattito di altissimo livello scientifico: spaziando dalle architetture tecnologiche alla gestione del fattore umano, la giornata ha saputo restituire un fedele quadro del panorama che vede gli operatori di cybersecurity (e non solo) lavorare quotidianamente alla costruzione del difficile ma necessario **dialogo tra accelerazione tecnologica ed esigenze di sicurezza**.

Come da tradizione l'evento si è concluso con la distribuzione gratuita ai partecipanti del ***bookazine*** **ICT Security Collection**, una selezione cartacea dei migliori contributi pubblicati nell'ultimo semestre dalla nostra omonima rivista online.