

*Il tema è stato al centro di una giornata di lavori (riservata soprattutto ad enti e imprese del settore tecnologia e telecomunicazioni) organizzata presso la sede romana del Cnr da quest'ultimo assieme ad Anitec e Cotec, con la partecipazione della Polizia di Stato. Tra i contenuti emersi, l'esigenza di poter controllare le reti di comunicazione a fini di sicurezza senza violare la privacy e la natura libera del web; il legame fra antispionaggio industriale e strategie antiterrorismo; l'impatto su cloud e big data. Comune denominatore e punto di partenza: l'importanza di rafforzare il rapporto tra l'industria, le istituzioni ed il mondo della ricerca*



Roma, 13 gennaio 2016 – La cybersecurity è un tema che sta assumendo sempre maggiore rilievo, in un'epoca in cui l'esigenza di controllo delle reti informatiche per ragioni di sicurezza pubblica si incrocia con la necessità di gestire reti di comunicazione strategiche per lo sviluppo economico e l'offerta di servizi innovativi.

Per questo Anitec, l'associazione confindustriale del settore Ict ed elettronica di consumo, assieme al Consiglio nazionale delle ricerche, a Cotec – Fondazione per l'innovazione tecnologica, con la collaborazione della Polizia di Stato ha organizzato una giornata di lavoro e confronto riservata alle imprese dell'Ict e delle telecomunicazioni. L'appuntamento si è tenuto il 13 gennaio a Roma, presso la sede del Cnr.

Tra le personalità intervenute Cristiano Radaelli, presidente Anitec, Luigi Nicolais, presidente Cnr e Alessandro Pansa, prefetto, capo della Polizia, direttore generale della pubblica sicurezza.

I principali temi affrontati sono stati: sicurezza delle reti, cyberattacchi e crittografia per la cybersecurity; sicurezza dei dispositivi mobili e dei sistemi di cloud computing; sicurezza dei software; gestione del rischio e della sicurezza dei sistemi; big data e condivisione delle informazioni nel rispetto della privacy; aspetti di informatica forense.

Per Cristiano Radaelli “le informazioni, assieme al capitale umano, sono il patrimonio principale di

imprese e organizzazioni. Per questo la loro gestione e la loro sicurezza rappresentano una priorità che, nell'era dell'Internet of everything, si traduce nell'esigenza di valorizzare sempre più figure professionali come data scientist, chief technology officer, sviluppatori mobili, big data architect. A livello europeo, le professioni Ict sono date in crescita del 27%. Il mercato della sicurezza informatica, in particolare, è fiorente ed è destinato a crescere da 75 miliardi di dollari di valore generato nel 2015 a 170 nel 2020. Più di 209.000 posti di lavoro nel campo della sicurezza informatica negli Stati Uniti sono attualmente vacanti e si prevede che la domanda mondiale sarà di 6 milioni entro il 2019, con un deficit previsto di 1,5 milioni. Per questo, l'emergere dirompente del tema della cybersecurity rende ancora più evidente questo scenario”.

“Per governare questo sviluppo e creare valore nel nostro Paese – conclude Radaelli – è necessaria la collaborazione tra imprese, centri di ricerca e forze dell'ordine. Il nostro Paese ha le competenze e le risorse per svolgere un ruolo importante per la difesa interna ed anche per fornire tecnologie e applicazioni ai Paesi e alle organizzazioni amiche. L'avvio della collaborazione tra Anitec, Cnr, Cotec e Polizia di Stato è una tappa importante in questa direzione”.

Come illustrato da Luigi Nicolais, “il tema della cybersicurezza, fino a pochi anni fa argomento prossimo alla fantascienza, oggi è uno degli asset strategici in ogni organizzazione su cui si concentrano investimenti in infrastrutture tecnologiche, sviluppo di competenze, definizione di profili professionali. È un settore in continua evoluzione destinato a crescere esponenzialmente e che pone intriganti sfide culturali e politiche. Mentre nei settori produttivi gli ambiti di intervento sono abbastanza definiti soprattutto laddove si opera in funzione di un obiettivo ben definito e circoscritto, la cybersicurezza sociale tocca ambiti molto più ampi, delicati e problematici perché investe la sfera dei diritti del singolo. È quindi opportuno che su questi temi non ci siano deleghe in bianco, ma che tutti, soprattutto se preposti ad assumere decisioni collettive, siano parte attiva”.

Il capo della Polizia, direttore generale della pubblica sicurezza, prefetto Alessandro Pansa ha dichiarato: “La complessità della tematica della cybersecurity impone oggi un inevitabile sforzo sinergico per soddisfare la quotidiana esigenza di sicurezza informatica. Per questo motivo la Polizia di Stato ha avviato una serie di collaborazioni per creare una rete di partnership, mettendo altresì a disposizione la propria competenza esclusiva del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.C.), quale organo di eccellenza per la fornitura dei servizi di sicurezza per le infrastrutture critiche”.

A partecipare all'iniziativa i rappresentanti di Accenture, Adb, Ads, Alenia Aermacchi, Almagora, Centro Fiat, Cisco, Cliocom, Comdata, Crf, Enac, Enel, Ericsson, Eustema, Facilitylife, Fastweb, Finmeccanica, H3G, Hewlett Packard Enterprise, Ids, Italtel, Microsoft, Nokia, Selex-es, Selta, Sitael, SmOptics, System Management Srl, Telecom, Thales Alenia Space, Università di Modena e Reggio Emilia, Vitrociset, Vodafone, Welcome Italia spa.

*fonte: ufficio stampa*