MASTER UNIVERSITARIO di II Livello

in

HOMELAND SECURITY

Università Campus Bio-Medico – Roma

Consorzio NITEL

PROJECT WORK

Definizione di un percorso formativo per decisori non tecnici in materia di cyber security; riferito agli aspetti strategici, tecnologici, organizzativi, legali e civili.

Relatore: Dott. Daniele De Nicolò

Tutor: Dott. Andrea Zapparoli Manzoni

ABSTRACT TESI

I grandi sviluppi tecnologici avvenuti negli ultimi decenni e le opportunità concesse da internet hanno avuto un profondo impatto sul modo in cui sono organizzate le nostre società e hanno ridisegnato la nostra vita di tutti i giorni, il modo in cui vengono condotti gli affari e le interazioni tra le persone. Oggi, molti aspetti della nostra vita privata e collettiva sono almeno parzialmente mediati, gestiti e controllati da tecnologie digitali e informatiche, sempre più collegate tra loro in reti sempre più complesse.

Mentre lo sviluppo tecnologico, e l'informatizzazione, in particolare, hanno avuto indubbi effetti positivi, hanno anche permesso la nascita di nuovi tipi di attività criminali, come *phishing*, *pharming*, frodi con carta di credito, furto di identità, cyber spionaggio, *hacking*, elaborazione e diffusione di virus e *worm*, solo per citarne alcuni. I criminali hanno inoltre scoperto che internet può fornire loro approcci completamente nuovi alle precedenti forme di criminalità, come l'estorsione, il furto o lo spionaggio.

Nel mondo di oggi, l'incapacità di rimanere aggiornati sulle minacce, le tendenze e le tecnologie più recenti può portare a considerevoli perdite economiche, perdita di fiducia, o addirittura la perdita di vite umane.

Il centro della questione è che non possiamo permettere che i malviventi che operano online siano più informati e meglio armati delle persone che hanno il compito di garantire l'integrità, la disponibilità e la

riservatezza dei nostri dati. Data la complessità delle infrastrutture ICT attuali ed emergenti, tuttavia, i responsabili delle attività che dovrebbero garantire il funzionamento e l'integrità di queste reti sono spesso in ritardo, quando si parla di sicurezza. Informare, attrezzare ed addestrare adeguatamente gli *stakeholder*, pubblici o privati, ad una cultura della sicurezza, consente di concentrarsi meglio sulla prevenzione e non solo sulla reazione alla minaccia. Inoltre, visto che l'uso e lo sviluppo delle tecnologie informatiche è diffuso in tutti i settori e i livelli dell'ambito professionale, la sicurezza informatica deve essere vista come una priorità collettiva, piuttosto che come un settore di specializzazione.

Per far fronte a questa situazione, l'obiettivo generale di questo progetto è quello di promuovere direttamente la creazione e la sostenibilità di una forte cultura della sicurezza tra i soggetti pubblici e privati, e di migliorare direttamente e indirettamente lo stato della sicurezza ICT, attraverso la realizzazione di una serie di corsi di formazione che possano coprire una vasta gamma di argomenti, ma tutti concentrati sulla sensibilizzazione e la promozione di una nuova leadership di sicurezza, e sullo sviluppo delle capacità necessarie per rispondere rapidamente ed efficacemente alle cyber-minacce alla sicurezza.

I principali beneficiari del progetto saranno gli istituti o le organizzazioni che parteciperanno ai corsi di formazione e che collaboreranno con essi. I beneficiari indiretti saranno i settori pubblico e privato, la società civile e l'economia, che indirettamente saranno più sicuri grazie alla natura distribuita delle tendenze di internet e ICT.