Offrire ai giovani un percorso di formazione per elevare il grado di consapevolezza rispetto alle emergenti sfide e opportunità che emergono dall'uso di internet, sempre più centrali nelle strategie delle aziende private e della Pubblica amministrazione. Questo l'obiettivo della prima summer school italiana per l'introduzione alla Cyber Security, organizzata dalla Scuola Superiore Sant'Anna di Pisa, con il coordinamento scientifico di Andrea de Guttry, direttore dell'Istituto Dirpolis (Diritto, Politica, Sviluppo) in collaborazione con il Centro Interdipartimentale IT Center dell'Università di Pisa,

e con il sostegno di Microsoft Italia che partirà il prossimo 4 luglio e rivolta a 25 partecipanti, selezionati tra studenti neolaureati, laureandi di corsi di laurea in discipline sia umanistiche sia tecnico-scientifiche. Tre ulteriori studenti avranno l'opportunità di usufruire di una borsa di studio messa a disposizione da Microsoft Italia.

Il corso, articolato in 5 moduli (Lessico e stato dell'arte; Problematiche; Sfide future; Cloud Computing; Soluzioni), vuole fornire gli strumenti e le conoscenze di base utili ad elaborare una riflessione critica sul tema della cyber-security. Attraverso lezioni in aula, simulazioni e analisi di casi studio, i partecipanti saranno preparati a gestire, in azienda così come nella Pubblica Amministrazione, le principali criticità legate alle minacce della sicurezza informatica. 40 ore di formazione volte a fornire una panoramica completa sul tema della Cyber Security, in particolare, sulle rilevanti questioni di natura tecnica, organizzativa, giuridica, politica, etica e socioeconomica riguardanti la promozione della sicurezza del dominio cyber attraverso un approccio interdisciplinare, volto cioè a trattare di cyber-security secondo diverse ma complementari prospettive.

Il progressivo sviluppo di Internet ha determinato la creazione di uno scenario economico avanzato che fa leva su infrastrutture e servizi erogati principalmente tramite un sistema di interconnessioni informatiche. La crescente diffusione delle tecnologie - Cloud, device mobili, Big Data analytics e IoT - ha portato enormi cambiamenti e benefici in termini di produttività, efficienza, oltre che vantaggi ai singoli cittadini, ma ha inevitabilmente cambiato lo scenario della sicurezza: l'impatto di minacce o semplici incidenti informatici può avere oggi una portata significativa, non solo in termini di disservizi per i singoli cittadini, ma di importanti ricadute di profilo economico, sociale, organizzativo, oltre che in termini di sicurezza a livello personale e globale (le minacce sono aumentate al ritmo del +30% nei primi 6 mesi del 2015 - CLUSIT).

L'attenzione al tema della Cyber-security negli ultimi anni si è fortemente sviluppata, sia in virtù di una maggiore consapevolezza dei rischi e dei danni generati dagli attacchi informatici che di vincoli normativi sempre più stringenti che costringono imprese e pubbliche amministrazioni a proteggersi e prevenire gli incidenti. Secondo gli ultimi dati dell'Osservatorio Information Security & Privacy - School Of Management del Politecnico di Milano, nell'86% delle imprese la consapevolezza dell'importanza di una gestione dell'information security & privacy è cresciuta negli ultimi tre anni; dato confermato anche dalla pianificazione del budget, che prevede nel 74% dei casi un'allocazione formale con orizzonte annuale o pluriennale.

Per affrontare in maniera efficace le minacce che, secondo quanto evidenziato dall'Osservatorio Information Security & Privacy, possono provenire tanto da fonti esterne come le organizzazioni criminali (nel 58% dei casi) o gli hacktivist (46%), quanto quelle interne, come

gli stessi dipendenti (49%) ed i consulenti aziendali (30%), occorre dotarsi di strumenti di protezione (firewall, antivirus, ecc.), ma soprattutto delineare politiche di sicurezza, basate sull'analisi dei rischi e sullo sviluppo di misure di protezione in linea con i potenziali pericoli e le esigenze delle singole infrastrutture, nella piena consapevolezza delle opportunità generate dallo "spazio cibernetico".

La diffusione di una cultura comune e condivisa della cyber-security tra gli individui, tra cui figurano i potenziali decisori politici, operatori economici e addetti alla sicurezza del domani, rappresenta un requisito imprescindibile per poter affrontare le sfide e cogliere le opportunità presenti e future che questo nuovo dominio offre.

Tutti i dettagli del corso sono disponibili su http://www.santannapisa.it/it/formazione/corso-di-formazione-su-introduzione-alla-cyber-security .