Progetto UNILAB - SEMINARI DI ORIENTAMENTO 2020

TITOLO: **Trasformazione digitale, Cybersecurity, protezione dei dati**

Data: 08 ottobre 2020
Il Docente: Professoressa Elisabetta Zuanelli
Cattedra: Comunicazione Digitale
Manager: Dott. Federico Santi
Azienda: Security Practice Leader DXC
Settore: Cybersecurity
Profili professionali di riferimento: Consulente e auditor in risk assessment; Consulente in risk evaluation per infrastrutture critiche; Esperto in data analytics, architettura e classificazione dati; Responsabile e addetto ai SIEM/SOC; Esperto nei CERT/CSIRT istituzionali e aziendali; Titolare del trattamento dei dati; Data Protection Officer (DPO); Responsabile del trattamento

---

il Webinar di oggi dal titolo *Trasformazione digitale, Cybersecurity, protezione dei dati* viene introdotto dalla **Professoressa Emerita Elisabetta Zuanelli**, Docente di **Comunicazione Digitale e Nuovi Servizi Digitali**, **Direttore Scientifico** del Master in **Competenze digitali per la cybersecurity, protezione dei dati, privacy** presso l'Università degli Studi di Roma "Tor Vergata", primo esperimento nella formazione interdisciplinare finalizzato alle nuove professionalità del sistema della sicurezza e della protezione dei dati. Dal 2016, la Professoressa Zuanelli è anche Coordinatrice del Partenariato PP, nato dall'idea dell'Unione Europea di aggregare risorse provenienti dal mondo accademico, dal mondo delle istituzioni e dal mondo delle aziende, con la prospettiva di erogare un piano di formazione nazionale in cybersecurity, cyberthreat e privacy.
Partendo dalla nozione di economia digitale, la Professoressa sottolinea fin da subito che il nostro Paese ha bisogno di formazione sulla cybersecurity e la protezione dei dati. L'Italia si trova infatti diversi gradini indietro rispetto ad altri Paesi Europei in tema di digitalizzazione e di sicurezza digitale, sia nel settore privato sia nel pubblico. La cosiddetta trasformazione digitale, innescata dal rapido sviluppo del mondo dell'ICT, è diventata prorompente dal punto di vista dei servizi e delle applicazioni di cui noi tutti ci avvaliamo quotidianamente. Il processo ha avuto avvio con l'esplosione di internet negli anni '90 del secolo scorso.
Quando parliamo di economia digitale, però, non dobbiamo intendere esclusivamente l'uso dei diversi dispositivi connessi in rete e di cui tutti siamo regolarmente e quotidianamente fruitori e utilizzatori. L'economia digitale ha pervaso tutti i processi produttivi. Quando prepariamo il caffè con la macchinetta automatica, quando attiviamo una lavastoviglie o un forno automatico, quando chiediamo ai nostri assistenti vocali di accendere o spegnere le luci, quando scendiamo in strada e prendiamo un mezzo che ci porti nei nostri ambienti lavorativi, utilizziamo utensili e strumenti che, in qualche modo, sono gestiti da software. Inoltre, spesso questi oggetti sono connessi tra loro: è il cosiddetto *Internet of Things.*
Se indubbiamente questo ha portato e porta semplificazioni quotidiane, la contro-faccia negativa è che, potenzialmente, siamo sotto minaccia costante di cyber-attacchi. In altre parole, le tecnologie consentono opportunità straordinarie, ma espongono anche a rischi straordinari. A cosa dobbiamo concettualmente fare attenzione? In realtà, il tema è estremamente ampio e molto complesso. Per questo è necessario un processo di alfabetizzazione digitale, volto a incrementare la consapevolezza degli utenti circa i rischi e le possibilità di proteggere sé stessi e i propri dati.

Il Master *executive* **Competenze digitali per la cybersecurity, protezione dei dati, privacy**, tratta nei tre assi sulle competenze giuridico-normative, economico-gestionali e tecnologico-digitali le diverse prospettive della sicurezza e della protezione dei dati, con una componente di laboratorio di oltre duecento ore, lezioni teorico-applicative di soggetti istituzionali, accademici ed esperti aziendali per oltre trecento ore e lo sviluppo di *project work* e *stage* mirati per ciascun partecipante al Master.

La Prof.ssa Zuanelli invita a questo punto il **Dott. Federico Santi** ad illustrare le strategie di cybersecurity. Santi, attualmente in DXC, si occupa infatti di cybersecurity e protezione dei dati da molti anni e ha maturato esperienze operando a livello nazionale ed europeo per grandi multinazionali della consulenza come Deloitte, sviluppando competenze di tipo progettuale e consulenziale.
Un primo aspetto importante da comprendere – spiega l'esperto - è che le campagne di cyber-attacco sfruttano spesso un vettore, quale ad esempio un grande evento nazionale o internazionale, o piuttosto la pandemia stessa, come verificatosi con il COVID-19. Questo vettore o acceleratore è infatti qualcosa che crea una debolezza, in alcuni casi anche psicologica, creando per l'opportunità per chi progetta cyber-attacchi di sfruttare la bassa alfabetizzazione informatica di molti destinatari di una determinata comunicazione, o una sua loro urgenza o presunta tale.
Se ad esempio siamo preoccupati per il COVID-19, come presumibilmente siamo tutti, diventiamo più esposti a minacce e attacchi.
Analisi di questo genere sono quotidiane per chi si occupa di sicurezza informatica, motivo per cui gli addetti ai lavori in questo settore sono coinvolti in una formazione continua e multidisciplinare.
È infatti apprezzabile che il Master in *Competenze digitali per la cybersecurity, protezione dei dati, privacy* sia tenuto nella Facoltà di Economia e non in una Facoltà di Ingegneria informatica.
L'informatica, nella cybersecurity, è un mezzo. È il mezzo utilizzato da chi attacca ed è il mezzo utilizzato, in parte, da chi difende. Ciò non toglie il fatto che sia necessario un processo di alfabetizzazione informatica a partire dalle scuole superiori, afferma il Dott. Santi. L'informatica però, si fonda su logiche. E se non si comprendono le logiche, non si possono mettere a punto efficaci strategie di cybersecurity. Per questo motivo, in ambito aziendale, vi sono profili che non sono strettamente informatici ma che nascono con una impronta di altra natura in modo da avere una vista ampia e collaterale all'evento. I termini "attacco" e "difesa" sono pane quotidiano per chi si occupa di cybersecurity e protezione dei dati, ed entrare nelle logiche di comprensione di questi fenomeni richiede una vista allargata e multidisciplinare per definizione.
È difficile suggerire delle soluzioni in ambito di cybersecurity se non si comprende effettivamente il mandato che una determinata azienda o amministrazione pubblica svolge. Bisogna conoscere in modo approfondito i molti aspetti e le molte sfaccettature della questione cybersecurity e protezione dei dati. In ragione di tale complessità, il mercato del lavoro presenta un sostanziale sbilanciamento tra domanda e offerta di profili qualificati, per questo motivo diventa fondamentale un processo di formazione e sensibilizzazione che porti i giovani a sviluppare queste nuove competenze. Quella di difendersi è infatti un'esigenza molto sentita dalle aziende di consulenza in tema di cybersecurity e protezione dati, dalle grandi pubbliche amministrazioni, dalle grandi aziende ma anche dalla società vastamente intesa.