Cyber sicurezza, le aziende imparano a difendersi - Il Nuovo Terraglio

Redazione

I recenti attacchi alle grandi multinazionali e, in queste ultime ore, a migliaia di server in tutto il mondo, Italia compresa, riportano con urgenza il tema della cyber sicurezza.

UNIS&F fa partire il primo Executive Master in Cyber Security dedicato alle aziende del sistema Confindustria Veneto Est. Un corso di alta formazione sulla sicurezza informatica dedicato alle PMI del nostro territorio. La proposta arriva da UNIS&F, la società di servizi e formazione del Sistema Confindustria che opera nelle province di Treviso e Pordenone che da tempo segue le aziende anche su questa specifica tematica e che per la realizzazione del primo Executive Master in Cyber Security dedicato alle aziende del sistema Confindustria Veneto Est, si è avvalsa del patrocinio di Clusit (Associazione Italiana per la Sicurezza Informatica) e del Club Bit (Associazione di IT Manager del territorio).

“Quello che è successo in questi giorni a migliaia di server in tutto il mondo conferma come la cyber security sia diventata un elemento strategico per la difesa dei dati delle aziende”, spiega **Pasquale Costanzo**, direttore generale di UNIS&F. “Ecco perché diventa essenziale essere pronti, per prevenire innanzitutto e poi, in caso, per arginare i danni. Siamo arrivati alla definizione dei moduli formativi del Master dopo un lungo lavoro di confronto con una quindicina di aziende legate al Club Bit che volontariamente hanno partecipato a tavoli di lavoro mirati alla raccolta delle esigenze che interessano di più: gestione delle vulnerabilità, furto di credenziali, whaling, truffa bancaria, ransomware”.

La pandemia ha moltiplicato l’utilizzo della rete a qualsiasi livello, amplificando i rischi di minacce cibernetiche. Come evidenziato dall’ultimo rapporto Clusit, nel primo semestre 2022 in Italia sono stati registrati 1.141 attacchi gravi (+ 8,45 % rispetto al primo semestre 2021) con una media di 190 attacchi al mese, il valore più elevato mai registrato ad oggi.

E il conflitto russo-ucraino sta mettendo in evidenza le fragilità di molte infrastrutture. Anche il rapporto DESI 2022 parla chiaro: l’Italia è al 25° posto in Europa su 27 paesi come livello di competenze digitali.

Questo richiede che in azienda ci siano figure professionali specializzate ad affrontare gli attacchi con una competenza a 360° sui diversi aspetti che possono impattare sul business. Negli ultimi quattro anni si è verificato un cambiamento epocale nei livelli di cyber sicurezza al quale non è corrisposto un incremento sufficiente delle misure di difesa.

Oggi la figura del singolo hacker è stata sostituita da vere e proprie organizzazioni criminali dotate di grandi mezzi e in grado di mettere a segno attacchi a chiunque. “Il problema non è sapere “se” un’azienda verrà attaccata ma “quando” avverrà”, ha aggiunto Pasquale Costanzo. “I mezzi per attuare delle efficaci difese esistono, quello che manca è la competenza nell’adottare gli approcci tecnologici e di metodologia più idonei per proteggerci. Le aziende devono cogliere l’opportunità per ripensare e riorganizzare la propria sicurezza informatica a difesa dell’asset “immateriale” più importante cioè i propri dati. Anche in questo ambito diamo seguito al nostro impegno di far evolvere il sapere al saper fare, proponendo un master executive in cui le aziende potranno simulare l’incidente prima che avvenga, allenarsi alla gestione delle attività di remediation e soprattutto essere in grado di prevenire danni al loro business”.

Il Master

Articolato in 50 ore di lezione, prevalentemente da remoto, l'Executive Master in Cyber Security inizierà l'11 marzo per terminare il 22 aprile, preceduto da una tavola rotonda in programma per il 23 febbraio, on line, per presentare i numeri sulla cyber sicurezza in Italia e i contenuti dei due mesi di formazione. In "aula" si ritroveranno manager, consulenti ICT e chiunque gestisca o sia interessato alla sicurezza delle informazioni in organizzazioni aziendali. I posti a disposizione sono in totale 15, la risposta dalle aziende è già molto buona, tanto che si sta pensando di replicare. Tra i relatori spiccano i più grandi esperti italiani in campo di sicurezza informatica ma anche appassionati di tecnologie digitali.

Come si è evoluta la cyber security negli ultimi anni, la mitigazione dei rischi, i piani di remediation, l'importanza del fattore umano nella cyber security, il punto di vista dell'hacker: queste e molte altre le tematiche che verranno trattate, fino alla simulazione di un attacco informatico. Spazio anche alle testimonianze con alcuni casi aziendali tra cui Bit Ways e il Gruppo Piazzetta. "Il master tocca tutti temi fondamentali dando l'impostazione che piace a me – ha detto Daniele Bonato, ICT Manager dell'azienda di Asolo – ovvero non entrare troppo in tecnicismi che sono per gli esperti del settore ma formare IT e responsabili della sicurezza dei dati per apprendere dei modelli organizzativi e operativi da applicare per iniziare un percorso di miglioramento continuo di mitigazione dei rischi".

A coordinare i lavori, il comitato scientifico formato da: Gabriele Faggioli, Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica) e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano; Alberto Mercurio, responsabile delle attività sul digitale di UNIS&F che da 20 anni lavora a fianco delle oltre 3000 aziende associate al sistema confindustriale di Treviso e Pordenone nella sensibilizzazione, nella progettazione e nell'erogazione di formazione dedicata allo sviluppo IT per rendere le persone in grado di utilizzare al meglio l'informatica come strumento di lavoro quotidiano e Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie.

I relatori

I 10 moduli previsti dal Master verranno affrontati con il contributo di relatori tra i quali: Luca Bechelli, Information Security & Cyber Security Advisor; Cesare Burei: "nerd" prestato al mondo delle assicurazioni; Daniele Longo, docente e consulente in ambito legale; Luciano Macera: autorevole specialista di tecnologie IT e Cyber Security sia in ambito IT che OT; Alice Mini: Cyber Security Specialist; Giorgio Sbaraglia, consulente aziendale in materia di Cyber Security; Rocco Sicilia: Ethical Hacker, Cyber Security Advisor e virtual CISO; Emanuele Stefan, Ethical Hacker certificato; Claudio Telmon: Consulente e advisor nel campo della sicurezza e dell'audit ICT; Cristian Toffoletto: Ethical Hacker e Pen Tester certificato è specializzato nell'ambito della Offensive Security.