Cybersecurity Experience, a Milano uno spazio dedicato alla formazione sulla sicurezza informatica

MILANO, 26 febbraio 2021 – Microsoft Italia presenta la **nuova Cybersecurity Experience**, uno spazio dedicato alla formazione sulla sicurezza informatica e collocato all'interno del **Microsoft Technology Center** della Microsoft House di Milano, il centro esperienziale progettato per permettere ad aziende e professionisti di vivere scenari d'innovazione, che anche nell'ultimo anno non si è fermato e ha coinvolto oltre 500 realtà in attività di **approfondimento virtuale**. Grazie al supporto del **vasto ecosistema di partner Microsoft**, l'azienda punta a sensibilizzare grandi imprese, PMI e Pubblica Amministrazione, sulle minacce informatiche e a promuovere la consapevolezza degli strumenti disponibili per proteggersi, nonché del valore del Cloud Computing a supporto della resilienza. L'iniziativa rientra nel più ampio impegno per la formazione e la cultura digitale alla base del piano quinquennale **Ambizione Italia #DigitalRestart**, che prevede 1,5 Miliardi di dollari d'investimento in tecnologie e competenze per far crescere il Paese.

Perché la Cybersecurity Experience oggi? Il progetto nasce dal costante impegno di Microsoft su questo fronte e dall'analisi dello scenario che vede la sicurezza informatica come un aspetto prioritario di cui farsi carico per la trasformazione digitale e la crescita del Paese. Secondo l'ultimo **Digital Defense Report** di Microsoft, infatti, gli attacchi informatici stanno diventando sempre più sofisticati, perciò per le aziende private e pubbliche è fondamentale dotarsi delle competenze e delle tecnologie necessarie a contrastare le minacce e a garantire la continuità dei servizi anche in un

clima di costante attacco. Secondo i dati Microsoft spopolano il **furto di credenziali** e i **ransomware**, nonché il **phishing** quale principale vettore di attacco, utilizzato in circa il **70% dei casi**. E i gruppi criminali sono sempre più in grado di far evolvere rapidamente le proprie strategie sfruttando le aree di sensibilità del momento, come dimostrato dal celere aumento di campagne di phishing a tema Covid-19 nella primavera del 2020: secondo i dati del **Rapporto Clusit 2020** sulla sicurezza cyber, infatti, il tema **Covid-19 è stato sfruttato da oltre il 40% delle campagne di phishing** nel periodo tra febbraio e giugno. Un esempio è il caso del **ransomware FuckUnicorn**, che ha colpito le organizzazioni sanitarie italiane attraverso l'invio di e-mail con un link che indirizzava gli utenti a un dominio malevolo, clone del sito della Federazione Italiana Farmacisti.

In questo panorama di minacce in continua evoluzione, le aziende italiane dimostrano in media una scarsa maturità dal punto di vista della cybersecurity e, secondo i dati dell'**Osservatorio Cybersecurity & Data Protection del Politecnico di Milano**, nell'anno della pandemia e della digitalizzazione "forzata" di molte realtà italiane, **Error! Not a valid link.**, ma la crescita del mercato della Cybersecurity è rallentata: **19% delle grandi imprese ha ridotto il budget** dedicato alla **sicurezza informatica** e solo il **40% lo ha aumentato**. In linea anche i dati relativi alle **PMI**, tra le quali **solo il 22% ha previsto investimenti in sicurezza per il 2021**. Questi dati confermano ulteriormente l'importanza di diffondere la consapevolezza dei rischi legati agli attacchi informatici e promuovere la formazione, a tutti i livelli aziendali e in ogni settore. Un obiettivo che Microsoft intende perseguire in collaborazione con gli **oltre 10.000 partner** che, su tutto il territorio nazionale, aiutano le organizzazioni italiane di ogni dimensione e settore a cogliere i benefici del digitale a supporto della propria crescita.

La nuova Cybersecurity Experience si inserisce proprio all'interno di questo impegno, con l'obiettivo di permettere ad aziende e professionisti di vivere in prima persona l'esperienza di un cyber attacco, tramite una **dimostrazione immersiva, interattiva e altamente personalizzabile** in base al settore di appartenenza e al ruolo dell'interlocutore. Le organizzazioni potranno fingersi hacker in simulazioni virtuali e al contempo testare l'esito di alcune minacce, dal dipendente fidato che lavorando da remoto può ingenuamente incorrere in errori, al collaboratore che con dolo cerca di compromettere il patrimonio informativo aziendale, fino ad attacchi veri e propri a cura di cybercriminali. Parte del percorso esperienziale saranno anche attività di ***vulnerability* e *penetration test***, che oggi devono comprendere le architetture logiche oltre a quelle fisiche. Nelle simulazioni verrà quindi mostrato anche il valore di strumenti che sfruttano grandi quantità di dati e possono essere interpolati per generare metodologie che vadano alla ricerca di percorsi esposti e vulnerabilità. Nella Cybersecurity Experience verrà perciò spiegata anche l'importanza dell'**Intelligenza Artificiale e del Machine Learning** in questa logica, anche grazie a demo che illustrano, per esempio, l'integrazione nei sistemi Microsoft – Defender e Sentinel – delle soluzioni del partner esperto in sicurezza Cymulate, con l'obiettivo di offrire sempre più capacità di *threat intelligence* alle aziende. Molteplici altri **partner Microsoft** giocheranno un ruolo centrale nell'arricchire la gamma di applicazioni a disposizione dei visitatori per rendere l'esperienza sempre più completa e personalizzata.

"Lo scoppio dell'emergenza sanitaria ha portato molte aziende ad avviare rapidi percorsi d'innovazione, con l'obiettivo di abilitare il lavoro da remoto e garantire la continuità di business, senza però lavorare a un piano di transizione che tenesse in considerazione gli aspetti legati alla sicurezza informatica, un fattore che le ha rese bersagli facili dei gruppi criminali. Al contempo, la pandemia non ha fermato le

campagne malevole, come dimostrato dall'ultimo Rapporto Clusit, che ha registrato 850 attacchi noti solo nel primo semestre del 2020, con una crescita del 7% rispetto allo stesso periodo dell'anno precedente", ha dichiarato **Andrea Cardillo, Direttore del Microsoft Technology Center di Microsoft Italia**. *"Microsoft è da sempre impegnata ad offrire le massime garanzie di cybersecurity, ma le tecnologie da sole non sono sufficienti. È essenziale che aziende, istituzioni e policy maker si uniscano in uno sforzo comune per fare la differenza, collaborando e condividendo informazioni per promuovere una cultura digitale improntata alla sicurezza. Con la nuova Cybersecurity Experience intendiamo fare un altro passo in questa direzione aiutando aziende, pubbliche amministrazioni e professionisti a rimane aggiornati sul panorama delle minacce informatiche e sugli strumenti a disposizione per proteggersi".*