VareseNews

Quando un click può mettere a rischio un'intera impresa, a Glocal Univa affronta il "cyber crime"

Pubblicato: Venerdì 12 Novembre 2021

Con la tecnologia che ci permette di essere **iper-connessi** in qualsiasi momento, spesso in una sovrapposizione tra la sfera personale e lavorativa, oggi può bastare un **semplice click sullo smartphone di un dipendente** per compromettere e consegnare a **criminali informatici** dati di lavoro **di un'intera azienda.** Ma come nascono questi pericoli? E come permettere a imprese e a privati di **difendersi dagli attacchi informatici, sempre più all'ordine del giorno**? Per rispondere e affrontare queste domande a **Glocal2021 l'Unione degli Industriali di Varese** ha organizzato un panel dedicato alla "**cyber sicurity**", che, tra "falso senso di sicurezza" e maturità tecnologica, nell'era post-covid dovrà "**ripartire da zero**".

«Il cybercrime è la fonte della **terza economia mondiale**. Solo nel 2021 ha portato a una **perdita del 6% del PIL** – spiega **Filadelfio Emanuele,** responsabile di **cyber security alla Elmec** rispondendo, in dialogo con **Marco Castiglioni e Luca Massi,** alle domande di **Silvia Giovannin**i, social media manager di Univa e moderatrice dell'incontro.

In particolare, come sottolineato dal responsabile di CybergON, **il mercato italiano si distingue per essere un'eccellenza mondiale** (dall'informatica al design, passando per la ricerca) custodendo uno dei principali contenitori di **dati sensibili** per quanto riguarda le aziende, con una **media di 600 attacchi subiti**, questi almeno i numeri che le aziende hanno voluto comunicare, ma probabilmente si tratta solo della punta dell'iceberg».

Secondo Emanuele le aziende devono infatti essere consapevoli che **non esiste un livello di sicurezza informatica garantito al 100%** ma che comunque è possibile abbassare il rischio, a volte attraverso **semplici accortezze per superare il "falso livello di sicurezza",** come possono essere degli investimenti sulla comunicazione e soprattutto sul **riconoscimento dei pericoli**, dai link di "fishing" al corretto aggiornamento del **backup dei dati**.

«Senza un approccio strutturato è difficile proteggere il dato – sottolinea **Marco Castiglioni**, cofounder di Cubesys – e la protezione del dato è inevitabilmente la base di tutti i modelli di sicurezza». Ma se c'è un fattore che può mettere a rischio il dato, quello senza dubbio il **fattore umano**, come la **negligenza o la corruzione**, qualcosa di imponderabile per le macchine, che, "se parlassero tra loro, senza intervento degli esseri umani", lascerebbero i dati con più facilità al sicuro.

Tra gli esempi citati da Castiglioni sull'importanza del fattore umano quello che fa maggiormente riflettere è uno **studio inglese secondo il quale in molti casi «sarebbe sufficiente offrire l'equivalente in sterline di una serata al pub in cambio di una password**». L'utilizzo di **una password uguale per ogni portale** (dal profilo privato Facebook di un lavoratore all'accesso alla posta aziendale) e la conseguente sincronizzazione tra diversi account in unico dispositivo costituisce un altro fra i principali rischi per le aziende, una sorta di **cavallo di troia**: «Ormai la tecnologia unisce ogni aspetto della nostra vita – fa notare Emanuele e Luca Masi -. Sul nostro cellulare, lo stesso che inconsciamente diamo a nostro figlio per giocare con chissà quale app, sono salvati e memorizzati dati personali e di lavoro, oppure accessi bancari: a questo punto **può bastare un singolo attacco informatico** per consegnare

nelle mani di malintenzionati tutti i dati. Un altro caso è rappresentato da sms per il pagamento di presunti **dazi dogali:** si crede di dover ricevere un ordine via posta e invece con un click si dà accesso a tutti i nostri, partendo dalle **carte di credito**».

Per porre una soluzione al problema Univa ha così voluto stilare '**Il decalogo della sicurezza informatica nelle imprese'**, una guida, a cura di **Luca Massi, responsabile dell'area Sistemi informativi di Univa,** per avvicinare le imprese che ancora trascurano la sicurezza informatica. «Abbiamo individuato **dieci punti** più evidenti – illustra Massi – Se le azienda si approcciassero con attenzione a questi dieci punti avrebbe una visione del problema di sicurezza informatica molto più chiara e raggiungerebbe un livello di sicurezza più adeguato».

«Se un utente di un'azienda è vittima di fishing (ovvero la truffa informatica) **non deve aver paura o vergognarsi** a comunicarlo all'azienda **prima che il danno diventi irreversibile per l'intera impresa**. Un consiglio semplice ma da non sottovalutare è quello di fare manualmente le "**pulizie di primavera**": ovvero svuotare la cartella di posta, cancellando tutti quei dati di lavoro non più necessari».

Una questione dunque non solo tecnologica, ma soprattutto di **cultura, sensibilità, comunicazione interna ed esterna.** Come nel corso di una pandemia, come abbiamo imparato nell'ultimo anno e mezzo, ognuno **può infatti costituire un "vulnus"** e deve assumersene la responsabilità. Proprio per questo fondamentale diventa la presenza **di un esperto** che sappia **preparare tutta l'azienda** per riconoscere attacchi informatici o che sappia per tempo bloccare l'emorragia di dati e fermare l'espansione del danno, a **livello tecnologico, comunicativo e umano**, per poi **ripartire in sicurezza**.

di M.Tr.