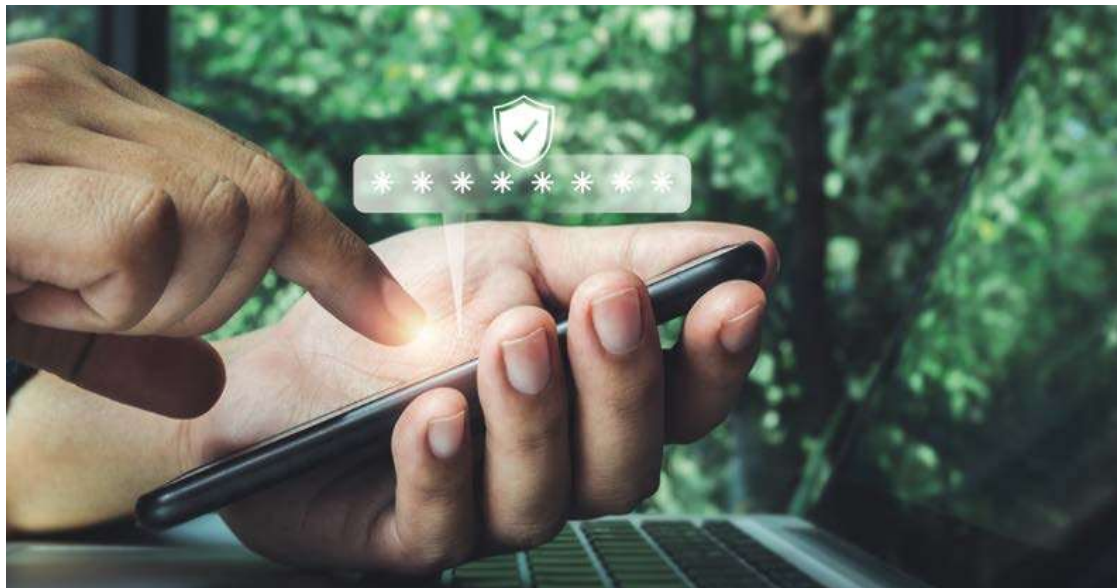


OPEN INNOVATION



Cybersecurity, la sensibilizzazione è la chiave

Una panoramica sulla sicurezza informatica



DI VINCENZO GERMANO*

Oggi più che mai il mondo fa affidamento sulla tecnologia, guardandoci intorno, la vita quotidiana dipende completamente da essa. I vantaggi di questa tendenza sono molteplici e l'accesso istantaneo alle informazioni su Internet ci consente di "navigare in un mondo" dalle infinite possibilità con un'immediatezza senza eguali, di conseguenza, la creazione di dati digitali è aumentata a dismisura, infatti, le persone ma anche le aziende e i governi archiviano una grande mole di dati sui computer/smartphone/cloud e li trasmettono attraverso le reti ad altri dispositivi. Ricavando enormi benefici dalla tecnologia, potrebbe essere difficile credere che potenziali minacce si possano annidare dietro ogni dispositivo, piattaforma, applicazione e programma utilizzato; eppure, nonostante la percezione "rosea" che abbiamo della tecnologia, le minacce alla sicurezza informatica sono un pericolo reale e

tangibile. Sentiamo sempre più spesso che la criminalità informatica è in costante aumento, mettendo in evidenza la problematica principale della tecnologia e costringendoci a chiedere cosa sia la sicurezza informatica – identificata come *Cybersecurity* –, perché è essenziale e perché è importante essere sempre informati per evitare spiacevoli situazioni. Se quanto appena detto lo riportiamo in un'ottica aziendale, la sicurezza informatica è fondamentale perché le organizzazioni di qualsiasi natura esse siano, raccolgono, elaborano e archiviano quantità senza precedenti di dati e molti di essi possono contenere informazioni sensibili, come dati finanziari, proprietà intellettuale, informazioni personali degli utenti e via discorrendo, per i quali l'accesso o l'esposizione non autorizzati potrebbe avere conseguenze negative. Questo perché i dispositivi e i relativi sistemi utilizzati presentano vulnerabilità informatiche che, se sfruttate a dovere, minano la salute e la stabilità di un'organizzazione. Per una qualsiasi azienda una

violazione di dati può avere una serie di conseguenze devastanti, basti pensare alla perdita di fiducia dei consumatori e dei partner nel caso in cui si venga a sapere pubblicamente di un "attacco andato a buon fine", oppure i server aziendali criptati completamente e inaccessibili se non dietro pagamento di somme di denaro in molte occasioni ingenti, oppure la perdita di dati critici, come file di progetti o brevetti, può costare a un'azienda il suo vantaggio competitivo impattando negativamente sui ricavi aziendali ma anche economico considerando la stima che in media una violazione dei dati può costare all'azienda interessata qualche milione euro. Se si pensa che già nel 2013, gli attacchi informatici e lo spionaggio digitale erano diventate la principale minaccia alla sicurezza nazionale, eclissando persino il terrorismo, con l'aumento del volume e della sofisticatezza degli attacchi informatici, le aziende, le organizzazioni ma anche i governi, è essenziale che adottino misure per proteggere le proprie informazioni sensibili e

implementino un solido approccio alla *Cybersecurity*.

DEFINIAMO LA CYBERSECURITY

Considerando le enormi moli di dati, tra cui anche dati sensibili, trasmessi attraverso le reti tra vari dispositivi, in estrema sintesi possiamo identificare la *Cybersecurity* come la disciplina dedicata alla protezione di tali dati ma anche dei sistemi, dei dispositivi, dei servizi utilizzati per elaborarli/archivarli, tesa a metterli al sicuro da criminali informatici, garantendo l'integrità, la riservatezza e la disponibilità delle informazioni. Perciò comprende un insieme in evoluzione di strumenti, approcci di gestione del rischio, tecnologie, formazioni e "best practice" progettate per proteggere reti, dispositivi, programmi e dati da attacchi o accessi non autorizzati. Questo perché generalmente gli attacchi informatici sono finalizzati all'accesso, alla trasformazione o alla distruzione di informazioni sensibili, nonché all'estorsione di denaro agli utenti e/o organizzazioni ma anche all'interruzione dei normali processi aziendali.

Il termine *Cybersecurity* viene utilizzato come onnicomprensivo per descrivere il processo di protezione contro ogni forma di criminalità informatica, dal furto di identità alle armi digitali internazionali; per quanto tale etichetta è valida, tuttavia non riesce a catturare la vera natura della sicurezza informatica per coloro che non hanno esperienza nel settore digitale, perciò è bene diffondere una cultura che possa informare il più possibile l'utente finale.

IL FATTORE UMANO

Oggi giorno l'implementazione di misure di *Cybersecurity* efficaci

è particolarmente impegnativa perché ci sono più dispositivi che persone, la complessità delle architetture di rete è elevata, i pirati informatici sono sempre maggiori, perciò azionalmente parlando si cerca di determinare e identificare il modo migliore per difendere tutte le risorse, dai computer e smartphone alle reti e ai database, dagli attacchi. Questo lo si fa identificando un "perimetro" ben definito sulla base del quale si studiano misure difensive ma le recenti iniziative e necessità di abilitazione come i lavoratori remoti, hanno dissolto il perimetro, ridotto la visibilità sull'attività informatica e ampliato la superficie di attacco.

Nonostante i livelli record di spesa da parte delle organizzazioni in ambito *Cybersecurity*, le violazioni sono in continua crescita e sempre più spesso le organizzazioni globali si stanno rivolgendo alla sicurezza informatica incentrata sull'uomo, ovvero un nuovo approccio che si concentra sui cambiamenti nel comportamento degli utenti finali anziché su un numero esponenziale di minacce crescenti. Tutto ciò si basa sull'analisi del comportamento degli utenti fornendo informazioni su come essi interagiscono con i dati in modo tale da estendere i controlli di sicurezza a tutti i sistemi in cui risiedono i dati. Perciò, in estrema sintesi, questo approccio è progettato per identificare le anomalie comportamentali al fine di far emergere e dare priorità alle minacce più gravi, riducendo i tempi di indagine e rilevamento delle minacce. Questo perché, indipendentemente dai dispositivi utilizzati, dai dati trattati, dai sistemi in essere, il fattore e la componente umana sono fondamentali, la sensibilizzazione verso gli strumenti utilizzati con un occhio attento alla *Cybersecurity* è sicuramente determinante.

CONCLUSIONI

Come appena analizzato, la *Cybersecurity* si concentra principalmente sulla protezione dei dispositivi e più in generale dei sistemi dagli aggressori, senza la figura fondamentale dei professionisti della sicurezza informatica che lavorano instancabilmente e senza solide difese, sarebbe facile perdere gli elementi essenziali moderni che fanno "funzionare il mondo", perciò, tra le altre cose, la *Cybersecurity* è di fondamentale importanza perché aiuta a preservare gli stili di vita che abbiamo imparato a conoscere e apprezzare.

***COMPONENTE COMMISSIONI INNOVAZIONE E INGEGNERIA FORENSE ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO**

HACKER O CRACKER

Costantemente i media utilizzano il termine *hacker* per identificare criminali digitali che mettono a rischio sistemi informatici commettendo qualsiasi tipologia di crimine informatico. Questo è profondamente sbagliato!! I pirati informatici, ovvero i criminali informatici non sono gli *hacker* ma bensì i *cracker*, spinti dalle più disparate motivazioni, dal guadagno economico allo spionaggio industriale, alle frodi o anche all'approvazione all'interno di una comunità di altri *cracker*, commettono qualsiasi tipologia di crimine digitale principalmente per un tornaconto personale. Al contrario gli *hacker* sono invece persone che con i mezzi a loro disposizione, si divertono a esplorare ed espandere (perciò non a manomettere) i sistemi informatici, cercando di far emergere le vulnerabilità, non per sfruttare come tornaconto personale, ma permettere la loro analisi e il loro miglioramento. Infatti, generalmente non lavorano individualmente ma in comunità, ritrovandosi periodicamente anche in meeting pubblici, considerano la condivisione dei saperi e delle informazioni un elemento fondamentale. Un esempio lampante sono i sistemi operativi Linux, che si sono evoluti negli anni in contrapposizione al colosso Microsoft, grazie a comunità enormi di *hacker*. Nella sua forma più generale, il termine *hacker* non si limita al solo campo informatico ma può essere utilizzato per identificare persone che non accettano passivamente le informazioni ma contribuiscono alla loro realizzazione, non limitandosi a imparare lo "stretto indispensabile" ma cercando di risalire alle origini dei problemi, al nocciolo delle questioni per trovare la soluzione più adatta espandendo il sapere mediante la condivisione.