L’importanza della Cybersecurity nei settori digitali

Data: Invalid Date | Autore: Redazione

La vulnerabilità delle organizzazioni a potenziali attacchi informatici è un dato di fatto. Molte imprese considerano le attività di “vulnerability assessment” e “penetration test" come meri adempimenti agli obblighi normativi o ai requisiti imposti dal settore di business a cui appartengono, ma in realtà si tratta di generare un vantaggio a lungo termine per la propria azienda.

Queste strategie sono solo un piccolo passo verso un processo di cybersecurity che si possa definire davvero avanzato.

Ovviamente non tutti i business hanno bisogno di strategie “forti” e dispendiose per il mantenimento della propria sicurezza informatica, ma è bene per tutte, anche le più piccole ed “immuni”, agevolare il processo osservando alcune regole base.

Quello che è però un dato di fatto è che la vita di ognuno è oggi più “digital”: si contano in media 6 ore al giorno ciascuno per l’intero corso della vita, spese online fra acquisti digitali, svago e intrattenimento soprattutto sugli innumerevoli siti, a partire da quelli meno comuni come le slots machine o ai videogame e sui portali streaming per la fruizione di film, Netflix e siti simili in primis. Infine, ma non per ultimi, i social network sui quali proprio le aziende hanno deciso di investire con il marketing digitale.

Sul digitale stanno poi investendo anche le Pubbliche Amministrazioni, le prime che dovranno adattare i loro sistemi a standard rigorosi di sicurezza informatica proprio perché deputate alla sicurezza del cittadino il quale le utilizzerà per erogare nuovi servizi virtuali. La sicurezza informatica per il settore digitale pubblico tocca infatti temi più vari come la privacy ed il trattamento dei dati

personali del cittadino.

La sfida non sarà quindi solo la transizione digitale in senso stretto, ma un processo più grande atto a mettere in sicurezza le migliaia di informazioni che verranno scambiate ogni secondo con i portali pubblici

Il ruolo dei consulenti digitali e perché è importante averne uno

Se sei un'azienda e tratti dati sensibili, sappi che adempiere ad alcune regole è di vitale importanza per difendersi da attacchi di hacking, oltre che essere un obbligo legislativo.

Come fare ad adempiere a tali regole? Innanzitutto essere seguiti da un consulente esperto in cybersecurity è la prima fase del processo di coinvolgimento di ogni aspetto del business, per essere coperti da ogni minaccia in ogni ambito.

Si comincia con i più basilari adeguamenti della parte IT e grazie ad un esperto questo diventa un processo semplice, alla portata di tutti. Gli step possono essere divisi sostanzialmente in due: il primo comprende l'analisi dei rischi, che verrà effettuata dall'agenzia di cybersecurity sulla base del business aziendale. I rischi potenziali non sono infatti per tutti uguali.

Il secondo step verte invece sui "security test", ossia tentativi studiati ad hoc per generare attacchi di hacking e testare dunque l'efficacia del proprio sistema di sicurezza informatica.

Perché la Cybersecurity e importante e quali ambiti deve coinvolgere per un'azienda che opera online

A sottolineare l'importanza della sicurezza in Rete, sono anche le iniziative italiane, come quella del "Cyber Secure City", iniziativa milanese che permette a privati e non solo, di generare nuove consapevolezze sul tema. Si tratta di un sito con dirette ed interviste esclusive che possono fornire un aiuto concreto a tutti coloro che si affacciano al tema per la prima volta. Sul portale è possibile trovare più di 80 ore di lezione che spiegano il perché è importante agire adesso.

Ma quali sono le suddette motivazioni? Innanzitutto come già detto, per un'azienda che opera con il proprio pubblico di riferimento scambiando dati personali, il tema è vasto e tocca anche quello della privacy e del nuovo GDPR. Ogni azienda deve infatti adempiere ad una serie di regole dettate dalla legislazione in materia, in caso contrario, a coloro che non si adattano, possono pervenire anche multe di decine di migliaia di euro.

Non meno importante poi, guardando al business personale, l'implementazione di sistemi di sicurezza avanzati che evitino agli hacker la facile sottrazione di dati, password e conseguenti perdite economiche ingenti. Pensiamo ad esempio ad un istituto di credito, ad una qualsiasi banca o servizio digitale che eroga fondi, prestiti, ecc., cosa può essere un'infiltrazione volontaria nei sistemi di sicurezza informatici aziendali. Importante in quest'ottica è fare un check anche di eventuali servizi di cloud, assicurandosi che questi dialoghino con la rete interna e non vi siano "fughe di dati".

L'integrità di un database aziendale si basa proprio sul controllo capillare di alcuni punti (touchpoint) di potenziale rischio, attraverso i quali un malintenzionato potrebbe infiltrarsi.

Ancora, per le piccole e medie aziende, moduli di pagamento, piattaforme digitali per la comunicazione e lo scambio di dati con il cliente potrebbero costituire un rischio concreto. Pensiamo a tutte le imprese medio piccole che si occupano di commercio elettronico o erogano servizi online, ad esempio. Infine, non meno importante, i software interni installati sui computer aziendali, come posta elettronica, interfacce per la comunicazione con enti vari, ecc… Questi potrebbero trasformarsi in veicoli per malware e arrivare fino ai dispositivi mobili ad essi collegati. I rischi spaziano dalla violazione di dati, alla condivisione di file impropri o spam.