

Cyber Security e Digital Marketing, serve una stretta collaborazione per proteggere dati sensibili e reputazione aziendale



Il Marketing è spesso considerato l'anello debole della sicurezza informatica. È tempo di ribaltare questa visione e creare uno stretto sodalizio fra gli esperti di Cyber Security e Digital Marketing per la definizione, diffusione e attuazione di strategie mirate a prevenire attacchi e a reagire opportunamente in caso di incidenti

Cyber Security e Digital Marketing sono ormai due facce di una stessa medaglia. Nell'era del **4.0** e dell'**Internet of Things**, infatti, i professionisti che lavorano in ambito **Marketing** si trovano spesso a dover gestire informazioni sensibili, collocate in ambienti **cloud** e diversificati, noti per essere maggiormente esposti ad attacchi informatici, interni e/o esterni. Quindi è

fondamentale che siano coinvolti nella definizione, diffusione e attuazione delle strategie di **Cyber Security**, non solo perché facile obiettivo per gli hacker, ma come soggetto attivo nel contrasto al **cyber risk**.

La **digitalizzazione** dei processi e dei sistemi informativi aziendali, ha consentito a molte organizzazioni di essere più competitive, ma questo ha significato, al tempo stesso, esporre i dati delle stesse a maggiori **rischi**. Di conseguenza la **Cyber Security** è diventata una **priorità assoluta** per le imprese.

All'interno di questo contesto, il **Marketing** è ancora percepito come un soggetto a rischio per la **sicurezza dei dati** di un'organizzazione e le persone che lavorano nelle posizioni di Marketing si sono abituate ad essere qualificate come anello debole dei sistemi di **sicurezza informatica**.

In realtà, preso atto che anche una sola violazione dei dati può danneggiare considerevolmente un'azienda, a livello di **Brand Reputation** e, in seconda analisi, di **costi economici**, nessuno può sentirsi al riparo da questo genere di minacce, qualsiasi sia la sua attività ed il settore in cui opera.

Questa riflessione assume un'ulteriore rilevanza se si considera che i trend digitali come **cloud**, **mobile**, **IoT** e **social**, ormai imprescindibili anche per le aziende, espongono le stesse a una grande quantità di **minacce**.

Per di più, l'opportunità di raccogliere una quantità di dati sensibili sempre più ampia, parliamo quindi degli ormai noti **Big Data**, aumenta ulteriormente la possibilità di **violazioni** di sistemi informativi aziendali.

Inoltre, gli **attacchi hacker** come il **furto di dati sensibili** dei singoli consumatori, la distribuzione di **malware** o l'**e-mail phishing**, sono spesso facilitati dall'incuranza e dalla scarsa conoscenza e consapevolezza del personale interno dei **rischi informatici**.

Pertanto è fondamentale che l'organizzazione, a tutti i livelli, **Marketing** incluso, sia **informata e consapevole** sull'importanza della **Cyber Security**.

Gli esperti di Cyber Security e Digital

Marketing devono collaborare di più

Ciò pone la domanda: cosa può fare il **team di Marketing** in tale scenario?

Data la quantità di **informazioni sensibili** a cui i **Marketer** hanno accesso e il crescente ricorso a **nuove tecnologie e ambienti digitali** per la condivisione interna e/o esterna all'organizzazione di questi dati, il Marketing è spesso obiettivo del **crime** sul web.

Perciò, in primo luogo, è essenziale **educare** le persone che lavorano in questo settore alla sicurezza informatica, con **percorsi formativi** creati ad hoc, per permettergli di identificare le specifiche tipologie di **attacco informatico** a cui potrebbero essere personalmente sottoposti, e ad usare con cautela ed intelligenza le **tecnologie digitali**.

Ciò significa anche che il Marketing dovrà comprendere l'importanza di collaborare con il **dipartimento IT**, per identificare eventuali minacce, rappresentate da nuove tecnologie, piattaforme e applicazioni, e determinare le misure di attenuazione del **rischio informatico**.

Una volta ridefinito il modo in cui i professionisti del Marketing affrontano il tema della **Cyber Security**, passando dall'essere facile bersaglio degli hacker, a utenti consapevoli dei rischi connessi al digitale, gli stessi marketer potranno essere d'aiuto all'intera organizzazione nell'arginare il **Cyber Crime**, diffondendo la **cultura della sicurezza informatica** tra tutte le funzioni in azienda.

Questo significa attivare campagne di comunicazione interna pensate per veicolare l'importanza della formazione sulla sicurezza informatica, contribuire alla diffusione del know-how aziendale riguardo le **best practice** in materia di **Cyber Security** e così via.

I Marketer devono essere pronti a

comunicare in caso di attacco informatico

L'obiettivo per i professionisti che lavorano in ambito Marketing è quindi quello di accelerare e diffondere l'adozione di una **strategia condivisa** sul tema della sicurezza informatica tra tutta la **popolazione aziendale**.

Ma il ruolo del Marketing potrebbe andare oltre l'attività di **diffusione interna** delle norme aziendali di **Cyber Security**. È infatti altrettanto importante che i **Marketer** siano preparati ad affrontare un eventuale episodio di **Cyber Crime** e definiscano quindi **preventivamente** un **piano di comunicazione esterna** in caso si verificasse un attacco informatico, così da evitare il panico tra clienti, fornitori e partner.

In definitiva, la **Cyber Security** è fondamentale ad ogni livello dell'organizzazione, così come la diffusione di una **cultura del rischio informatico** e, al tempo stesso, lo sviluppo di una **fiducia digitale**.

All'interno di questo scenario, il **Marketing**, anziché l'anello debole della **sicurezza informatica**, può costituire la prima linea di difesa contro il **cyber risk** e contribuire a cambiare la prospettiva dalla quale il personale interno guarda a queste tematiche, permettendogli di comprendere come oggi la **Cyber Security** ricopra un **ruolo abilitante**, e non frenante, rispetto al raggiungimento degli **obiettivi di business**.