La sicurezza sui Social Media per le PMI

Chi rinuncia alla libertà per la sicurezza, non merita né l'una né l'altra (B. Franklin): un principio applicabile anche alle aziende che usano i social network.

Alessia Valentini - 29 marzo 2013

Social Media in sicurezza

Al Security Summit 2013 di Milano, la community dei Partner **Oracle** ha spiegato alle aziende come utilizzare il Web 2.0 in piena sicurezza. Le PMI italiane, infatti, devono perseguire i vantaggi offerti da un uso intelligente dei social network, ma senza trascurare le minacce dei nuovi ambienti virtuali.

=>Come garantire la sicurezza nell'era Web 2.0

Allo scopo, è stato redatto un **white paper** sulla **Social Business Security** (SBS), con tutti gli aspetti rilevanti per proteggere gli asset materiali e immateriali e per una corretta gestione dei rischi.

Il **modello** proposto è un uso consapevole dei Social Media ("*Go social responsably*"): la SBS tiene infatti conto di politiche di ICT Security, Reputation Management, Brand Protection, Compliance, tutela legale, Open Source Intelligence (OSInt), Digital Marketing e altre discipline specifiche nate in ambito Social (es.: Conversation Management).

Le piattaforme social sono bersagliate da **minacce** quali malware, attacchi di social engineering, spam, phishing, furti di identità, proprietà intellettuale e dati sensibili, con il contestuale rischio di perdita o diffusione incontrollata di informazioni riservate e danni reputazionali.

Senza voler fare terrorismo viene insegnato come tutelare la propria impresa in modo pratico.

=>Guida al Social Media Scheduling per le PMI

Percezione della sicurezza

Dallo studio emerge una percentuale piuttosto alta (77,8%) di aziende favorevoli al **BYOD** e alla consumerizzazione dell'IT, tali da permettere l'utilizzo di device personali in azienda, l'accesso alla rete/applicazioni/web o ai Social Network. Eppure, nessuna possiede un sistema di Security **Assessment** dedicato, e solo 11% si sottopone regolarmente a Security **Audit**. Meno del 50% adotta **policy** specifiche per

i dipendenti, mentre il 67% effettua test di Vulnerablity Assessment, ma non sistematicamente.

Rischi

Gestire le minacce significa conoscerle con un approccio strutturato, catalogando quelle specifiche e valutandone l'impatto sul business, sfruttando al meglio le risorse disponibili. I rischi possono essere così classificati:

- **Conformità** – trattamento dati non conforme alla normativa vigente o alle politiche aziendali.
- **Operativi** – attività dei dipendenti condizionata dalla commistione tra dati personali e aziendali.
- **Relazionali** – danni al brand o all'immagine e insoddisfazione dei clienti.

Un rischio che deve essere valutato in modo appropriato è l'utilizzo dei social da parte di terzi altri in merito alla propria azienda: pubblico, consumatori, dipendenti e collaboratori, quando non malintenzionati e concorrenti. In questo senso, l'obiettivo dell'azienda deve essere la **Social Media Neutrality** (azioni da intraprendere, anche senza usano attivamente gli strumenti social).

=>Scopri come garantire la sicurezza sul Web

Contromisure

Istituire forme di contrasto efficaci richiede un **intervento sinergico**: attività di tipo culturale e organizzativo, soluzioni di carattere processuale, procedurale e tecnologico. L'applicazione parziale e/o non coordinata delle contromisure risulta inefficace.

In azienda è necessario coinvolgere i reparti IT, Sicurezza, Marketing e Legale con attività di formazione e aggiornamento, definendo regole chiare e condivise, per l'utilizzo dei Social Media, misurando adozione ed efficacia nel tempo. In pratica, una Social Media Policy arricchita dalle competenze dei ruoli aziendali coinvolti nelle iniziative che l'azienda persegue online.

Sul Web bisogna gestire la presenza attiva e passiva dell'azienda nei Social Media. Gli utenti devono essere responsabilizzati ad usare la moderazione per prevenire incidenti (danni alla reputazione, perdita di dati, involontaria attivazione di codice malevolo), per governare eventualmente i quali devono essere predisposti processi e team di "gestione crisi": l'istituzione di procedure guidate aiuta a non commettere errori e a non improvvisare.

Infine, è fondamentale adottare **strumenti di monitoraggio** che possono in automatico prevenire, individuare ed eventualmente bloccare potenziali minacce.

Lo studio si conclude con alcune case histories che permettono di comprendere come sviluppare il business aziendale e contemporaneamente mantenerlo al sicuro.

*Per richiedere il documento visita questo **link***

Se vuoi aggiornamenti su **LA SICUREZZA SUI SOCIAL MEDIA PER LE PMI** inserisci la tua e-mail nel box qui sotto: