La Sicurezza nei Social Media [Intervista]

Scritto da: Sonia Montegiove 8 aprile 2013 in InWeb 2.0 6 Commenti

Parliamo spesso di quanto sia importante per le aziende cogliere le opportunità che offrono i Social Media. Non solo bisogna saperci stare, e non solo esserci, ma bisogna anche avere ben presente quali siano i rischi. Ne abbiamo discusso con Mauro Alovisio e Andrea Zapparoli Manzoni, co-autori de "La sicurezza nei social media", un interessante documento prodotto da Oracle Community for Security

"La nostra posizione è univoca: raccomandiamo fortemente alle imprese italiane, in particolare quelle del Made in Italy, di **usare i social network, in quanto essi rappresentano una reale opportunità, ma di farlo in modo intelligente e informato**". Questo è quello che si legge nella presentazione di "**La sicurezza nei social media**", un interessante documento prodotto da **Oracle Community for Security,** interdisciplinare ed edito creative commons, scaricabile gratuitamente all'indirizzohttp://social.clusit.it/views/Social/Homepage.html, che vuole puntare l'**attenzione sulla sicurezza**, tanto più minata quanto più le aziende, e non solo, si affacciano sui social network. Il lavoro non mette in evidenza soltanto i rischi con l'intento di far acquisire quella consapevolezza che ciascuno dovrebbe avere affacciandosi in Rete, ma fornisce dei consigli pratici per la tutela propria e dell'azienda dal punto di vista legale e informatico. **Abbiamo posto qualche domanda a due dei coautori del documento: l'avvocato Mauro Alovisio** per la parte giuridica e **Andrea Zapparoli Manzoni per la parte informatica**.

Qual è la raccomandazione inerente la sicurezza più disattesa dalle aziende e perché?

> *Nella nostra esperienza gli errori più comuni e con il più alto tasso di rischio compiuti dalle aziende sui Social sono (in ordine di frequenza):*
>
> 1. ***non preoccuparsi della Net Neutrality****, cioè non partecipare ai Social e non tenere sotto controllo la propria identità digitale, rischiando così il* ***Brand Hijacking*** *(che può avere conseguenze molto gravi, trattandosi di PMI e micro-imprese)*
>
> 2. ***non affidarsi a professionisti****. Il fai-da-te, che purtroppo è estremamente diffuso soprattutto in ambito PMI, è quasi una garanzia che si subiranno incidenti. Non mi riferisco solo alla necessità di avvalersi di esperti di Social marketing (che anzi spesso sono più*

"spericolati" dei loro committenti!), ma anche e soprattutto ad altre figure che dovrebbero concorrere nel supportare un'azienda che utilizzi i Social (a qualsiasi titolo), in particolare legali ed esperti di ICT Security.

3. ***gestire gli account social tramite una macchina utilizzata anche per altri fini****(come ad esempio amministrativi, di segreteria o per utilizzi personali del titolare). Questo comportamento è decisamente poco "igienico", dal momento che espone l'intera organizzazione ad ogni sorta di attacco e compromissione (antivirus e firewall sono praticamente inefficaci, ed anche un eventuale sistema di web content filtering ormai serve a poco). Porto un caso successo di recente: un'azienda mi ha contattato per un attacco veicolato via social, a causa del quale ha perso tutti i propri dati amministrativi (inclusi i backup) in quanto cifrati dai cybercriminali, che ora chiedono 50mila dollari per "liberarli". Dal momento però che la gang in questione è appena stata sgominata dall'Europol, l'azienda non può nemmeno pagare il riscatto e sono impossibilitati a lavorare.*

4. ***non moderare la conversazione*** *(o comunque non farlo in real-time). Mi rendo conto che, per volumi di conversation medio-alti si tratta di costi non indifferenti, d'altra parte è l'unico sistema che garantisce un buon livello di sicurezza (sia informatica, relativamente a dati ed infrastruttura, che degli asset immateriali come la reputazione) e che consente di ridurre al massimo l'impatto degli incidenti di data leakage.*

5. ***esporre i propri clienti, utenti, followers, partners ad attacchi a causa della mancata gestione dei rischi*** *che conseguono dai punti 1-4 (il che configura scenari di liability).*

Perchè le aziende compiono questi errori?

Dal lato della domanda:

- ***errata percezione dei rischi / mancanza di awareness***
- ***mancanza di un budget dedicato*** *(anche in base all'idea balzana secondo la quale Internet, ed i Social in particolare, sono "gratuiti")*

Dal lato dell'offerta:

- ***scarsità (almeno fino ad oggi) di soluzioni ad-hoc*** *ritagliate sulle esigenze e sulle disponibilità delle PMI.*

Nella guida si raccomanda la lettura dei Terms Of Service. Ma quanti non "addetti ai lavori" sono in grado di comprenderne il contenuto? Cosa si potrebbe fare secondo te per renderli più comprensibili?

Le social media policy esterne ed interne *per essere efficaci non devono essere calate dall'alto e non devono essere strumenti rigidi ma al contrario devono essere* ***elaborate con***

meccanismo bottom up e devono essere condivise dai diversi uffici dell'impresa *(comunicazione, marketing, personale, sistemi informativi e non solo da giuristi) anche al fine di accrescere il senso di appartenenza all'organizzazione e la forza del brand.*

Si suggerisce pertanto una ***coralità di azione e di competenze aziendali****; occorre scrivere****poche cose in termini chiari e trasparenti non una serie di noiosi e impraticabili divieti****: l'ottica deve essere di inclusione dei cittadini e dei consumatori, di accrescimento reciproco e di consapevolezza delle potenzialità e dei rischi dello strumento social media utilizzato. Occorre pertanto lavorare per punti sintetici anche a livello grafico e monitorare il livello di comprensione e di interesse per il testo.*

Si suggerisce inoltre ***testare il grado di chiarezza del testo della social media policy*** *con alcuni test preliminari prima della messa on line e verificare anche i profili dell'accessibilità anche dai cellulari.*

Molteplici social media policy presenti on line nelle pagine delle piattaforme trascurano i profili strategici dell'utilizzo del marchio, logo aziendale e del brand; il profilo di indicazione di contatti aziendali di prevenzione del contenzioso in materia di diritto d'autore e la presenza delle traduzioni in più lingue.

Nella redazione della social media policy occorrerebbe ***conoscere bene il target al quale ci si rivolge****, il piano di comunicazione dell'impresa dell'azienda e le priorità strategiche della governance in materia di comunicazione (es. priorità su questionari on line di gradimento servizi; su lancio di nuovi prodotti, su concorsi a premi, su campagna saldi stagionali etc..).*

Occorre inoltre tenersi ***costantemente aggiornati sulle condizioni legali di utilizzo dei social media e sulla giurisprudenza evolutiva*** *comparata ad esempio in materia di diritto all'immagine, diritto di autore etc.*

Le social media policy devono inoltre essere aggiornate costantemente; si tratta di un processo di apprendimento continuo sia da parte dell'impresa sia da parte degli utenti.

Il logo utilizzato per caratterizzare il documento – frutto della collaborazione di una trentina tra aziende, studi legali, consulenti direzionali e associazioni – è una ciliegia. Perché **i social network sono attraenti e apparentemente solo gustosi come le ciliegie. Ma come esse nascondono l'insidia del nocciolo, non solo spiacevole da addentare ma estremamente pericoloso**. Soprattutto per chi non ne conosce l'esistenza.