www.ecostampa.it

TechVIDEO.tv by DATA MANAGER Il punto di riferimento nei video ICT
Il meglio della tecnologia cliccando PLAY

LA CLASSIFICA DELLE SOCIETÀ DI SOFTWARE E SERVIZI IN ITALIA Edizione 2012

paper.li

Social Media e Security

15/03/2013 | a cura di Redazione Data Manager Online

Mi piace 5 | Invia | Share 2 | Tweet 5 | +1 2

DataManager su Segui

+1 +243

A cura di Luigi Pachì

In un incontro avvenuto al recente Security Summit di Milano, il Clusit, l'Aused e la Oracle Community for Security, con l'obiettivo di far crescere la cultura della sicurezza in Italia, hanno presentato un white-paper (richiedibile tramite il sito http://c4s.clusit.it) sul tema della sicurezza nei Social Media. I contenuti raccolti rappresentano la summa eterogenea di 34 professional di Security (provenienti da 3 associazioni, 3 studi legali, e 16 aziende) che permette di avere una sorta di guida liberamente scaricabile all'uso della security dei social media.

Entrando nello specifico, e riassumendo l'argomento, i Social Media rappresentano oggi una ciliegia, rossa e matura, pronta per essere addentata. Ma, attenzione: chi mangia le ciliegie deve anche stare attento al nocciolo!

Voglia di Geomarketing ?

GeoLAND esegue analisi del territorio, valutazioni di punti di vendita, valuta la concorrenza e mostra le caratteristiche del mercato assegnato ad ogni agenzia.

Ora Su TechVIDEO.tv

Codemotion 2013. Videointervista a Emanuela Zaccone Co-founder di AIDA Monitoring

Codemotion 2013 - MAKERS. Videointervista ad Antonio Ianiero di Unterwelt

Codemotion 2013 - MAKERS. Videointervista a Simone Tibollo di Field Effect Labs

VEDI TUTTI ››

smau PADOVA 17-18 APRILE

028941

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

www.ecostampa.it

Premettendo che i Social permettono molteplici opportunità di business e sono strumenti di marketing molto utili e potenti per le aziende, dobbiamo però, in questo contesto odierno, focalizzarci sul tema della sicurezza e sulle eventuali minacce che ne derivano.

La realtà che emerge è che i Social Media nelle aziende vengono sempre più utilizzati, ma esiste una scarsa presenza del tema Security e molto spesso non esiste una policy adeguata. Nell'ambito di un questionario sulla gestione e percezione della security in ambito Social Media presente nel white-paper presentato durante l'incontro, risulta chiaramente che, sebbene vi sia una percentuale piuttosto alta (pari al 77,8%) che consente l'utilizzo di device personali in azienda per accedere alla rete/applicazioni/web, o che lascia libere le persone di accedere ai Social Network, di contro abbiamo percentuali dello 0% alla domanda: "Avete un sistema di Security Assessment dedicato ai Social Media?", oppure del solo 11% alla domanda: "I fornitori di soluzioni marketing Social Media e Web, nel caso di forniture SaaS, sono sottoposti ad un Security Audit?". Meno del 50% delle società che hanno partecipato al sondaggio ha una policy per i dipendenti relativa ai Social Media, mentre una percentuale più alta – anche se non del tutto rassicurante – dimostra che il 67% effettua test di vulnerablity assessment.

Il concetto di fondo è che oggi, con l'avvento dei Social Network, si rischia a prescindere; non importa se si è parte o se si è completamente fuori da questi, perché chi guida il flusso di informazioni a favore o contro una azienda o persona può essere chiunque. Passare dal mondo virtuale del social a quello reale della borsa è davvero un attimo, anche con conseguenze disastrose.

Per esempio, una nota catena americana di pizzerie, nell'aprile 2009, ha subito un brusco calo di vendite, in ragione della pubblicazione su YouTube di un video da parte di due suoi dipendenti.

In questo video i due impiegati mostravano le loro molteplici violazioni di regole igienico-sanitarie durante la preparazione di un pasto. L'effetto del video, di enorme diffusione su YouTube, è stato amplificato dal fatto che la reazione della compagnia è avvenuta solo alcuni giorni dopo la pubblicazione dello stesso, causando inoltre all'azienda un calo del 10% in market capitalization nel periodo immediatamente successivo all'accaduto. Esempi più recenti sono le recensioni su TripAdvisor che, se scritte volontariamente in modo malevolo, possono condurci nel farci desistere dallo scegliere un hotel, o un ristorante, ecc.

I fattori moltiplicativi portano potenzialmente a coinvolgere nel chiacchiericcio dei Social Media l'intera popolazione dei consumatori finali e delle imprese: per questo non si può ignorarlo. Si può licenziare un dipendente ma non un consumatore, si può far causa a un concorrente sleale ma non a un filmato, a un post, a un click. Da sempre i consumatori parlano dei prodotti e delle aziende che li producono, da sempre i

028941

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

www.ecostampa.it

Social Media l'intera popolazione dei consumatori finali e delle imprese: per questo non si può ignorarlo. Si può licenziare un dipendente ma non un consumatore, si può far causa a un concorrente sleale ma non a un filmato, a un post, a un click. Da sempre i consumatori parlano dei prodotti e delle aziende che li producono, da sempre i dipendenti parlano e sparlano dei capi, dell'azienda, per cui lavorano, del lavoro che fanno: i Social Media rendono la piazza globale, fanno sì che il chiacchiericcio coinvolga tutti e raggiunga tutti gli angoli della Terra.

I Social Media sono un fenomeno intrinsecamente "consumer", non sono un fenomeno dominato o finanziato dalle imprese; esistono e si diffondono secondo percorsi difficilmente prevedibili e influenzabili dalle imprese.

E' evidente che in questo contesto ogni azienda (ogni persona) può essere coinvolta inconsapevolmente dai Social Media. Questo perché qualcuno parla dei suoi prodotti o perché scelte aziendali provocano reazioni sociali (lavoro, ambiente, salute…), ma anche perché l'azienda è una appartenenza comune dei suoi dipendenti, o fornitori, o clienti, e dunque un elemento passivo di aggregazione.

I Social Media, per altro, non sono facilmente inquadrabili sotto il profilo legale, sia da un punto di vista legato alle responsabilità, che del Foro competente e della Giurisprudenza.

E tra i vari problemi che emergono occorre ricordare che la presenza passiva nei Social Media non è evitabile e può provocare danni significativi.

Ma analizziamo alcuni rischi intrinsechi senza che l'azienda abbia fatto nulla, o che l'azienda non ne sappia nulla. Prima di tutto, quando la concorrenza sleale capisce il fenomeno, nasce un nuovo rischio di business. In seconda analisi, un consumatore insoddisfatto, un dipendente arrabbiato possono trasformarsi - a costo zero - in un rischio reputazionale verso tutti i clienti.

Il nuovo rischio non riguarda solo le grandi aziende, i grandi marchi: per esempio una pensione romagnola contro un'altra (per tornare all'argomento della scelta degli alberghi con Trip advisor),

oppure un ristorante invece di un altro (consultiamo i pareri dei clienti prima di scegliere? Chi ci dice che alcuni di quelli che leggiamo negativi non siano stati inseriti dal ristorante concorrente?)

Le community, i gruppi spontanei, le chat, i blog che parlano dell'azienda o dei bisogni che i prodotti dell'azienda risolvono (salute, alimentazione, bambini…) o che organizzano le relazioni tra colleghi (l'aperitivo, la partitella, l'azione sindacale…), target preferenziali per le attività di Social Engineering, possono diventare veicoli inconsapevoli di informazioni riservate, indirizzi di e-mail, organigrammi, di appuntamenti o garanti di reputazioni false. E anche in questo caso senza che l'azienda

028941
Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

www.ecostampa.it

Questione di consapevolezza

Per gestire quanto sopra c'è un costo da sostenere per contrastare i rischi derivanti dalla semplice esistenza dei Social Media. In primis, rendere consapevole l'azienda dei rischi e rendere consapevoli i propri dipendenti dei rischi impliciti nello strumento. Poi monitorare la presenza passiva (citazioni, riferimenti, notizie) e creare le condizioni per reagire in fretta e bene in casi di attacco o se si viene "bucati" su Twitter o altri social network. Questo costo è legato alla presenza passiva sui Social Media: viene prima e deve essere aggiunto ai costi dei progetti aziendali di presenza sui Social Media. Il ROI nei Social Media deve essere valutato al netto del costo della "presenza passiva" che possiamo definire "social media neutralità".

Ma facciamo ora un passo avanti, e vediamo i rischi di quando nei Social Network ci si trova non solo passivamente. Le caratteristiche dei Social Media che offrono alle aziende le maggiori opportunità e, dunque, esercitano la maggiore attrattiva, sono spesso i medesimi elementi che danno luogo ai maggiori rischi tecnologici. Un approccio strutturato alla gestione dei rischi, richiede innanzitutto una catalogazione dei rischi specifici, derivanti dall'utilizzo dei Social Media. I rischi generati dall'utilizzo dei Social Media in azienda sono molteplici, ma possono essere classificati secondo i seguenti cluster principali: rischio di conformità, operativo e relazionale. Nel primo dei tre cluster rientrano i temi di trattamento dei dati non conforme alla normativa vigente, il trattamento dei dati non conforme alle politiche aziendali, i rapporti con dipendenti e candidati e la commistione tra dati personali e dati aziendali.

Guardando invece l'aspetto operativo, ci troviamo davanti alla diffusione di malware, al furto d'identità, Phishing e Social Engineering, ma anche a rapporti con dipendenti e candidati, per non parlare di perdita di produttività, perdita di controllo sui contenuti e rischi operativi dei Social Media tramite dispositivi mobili. Infine, il terzo cluster, quello legato al rischio relazionale, vede al suo interno le voci che riguardano il danneggiamento del brand (danni all'immagine verso l'esterno), i danni all'immagine verso l'interno e l'insoddisfazione dei clienti.

Che trascurare la sicurezza non paghi risulta evidente dai molteplici casi critici che ci vengono sollecitati dalla stampa periodicamente. Si pensi al doppio attacco subito dalla Reuters nell'agosto 2012, quando a loro insaputa sono stati postati nella piattaforma di blogging false notizie attribuite a giornalisti Reuters legate alla propaganda del regime siriano. Oppure quando sono state rubate 6,4 milioni di password da LinkedIn (costringendo molti utenti a cambiare la propria password), o le 11 milioni di password rubate dal sito di giochi on-line Gamigo.

028941

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

www.ecostampa.it

La nuova era del consumismo, che vede operare sui Social il cosiddetto "consum-attore" porta a vedere i Social Media anche come strumento di ascolto. Resta comunque importante l'analisi dei dati, ricordandoci però che non esiste difesa alcuna quando si è inconsapevoli dei pericoli che si corrono. Il Garante ha realizzato un video dal titolo "connetti la testa" per far riflettere le persone su come usare i social network in modo sicuro e consapevole, ma sono soprattutto le aziende che devono decidere una strategia sui social media con regole da condividere al proprio interno; devono essere coinvolti tutti i ruoli aziendali, dal marketing, all'ICT, dal giurista fino al sociologo, se presente). Occorrono policy interne che indichino i responsabili del sistema, perché fare Social Networking significa anche creare velocità di reazione in azienda.

La necessità di azioni sinergiche

Finora abbiamo accennato ai potenziali rischi dei Social Media, ora proviamo ad affrontare le contromisure. Possiamo dire che è possibile agire in maniera sinergica su tre direttrici. La prima soluzione coinvolge attività di tipo culturale e organizzativo. Poi abbiamo soluzioni di carattere processuale/procedurale, e infine soluzioni di carattere tecnologico.

Guardando agli ambiti d'azione, le contromisure possono essere raggruppate in base al tipo di rischio da mitigare, in particolare al rischio operativo e al rischio relazionale.

Naturalmente l'applicazione parziale e/o non coordinata delle contromisure risulta inefficace.

Allo stesso modo, l'assenza di figure professionali adeguatamente preparate e di dialogo tra i manager delle diverse aree coinvolte (HR/IT/Security/Marketing/Legal) le rende poco incisive.

I Social Media non sono un problema (solo) dell'IT, e neppure un ambito di pertinenza esclusiva del Marketing.

In conclusione possiamo dire che per ottimizzare il ROI del Social Business, sia per evitare danni economici o d'immagine (anche importanti e complessi da sanare), sia per impedire la perdita di dati sensibili o per rimediare ove gli incidenti si siano già verificati, è necessario fare formazione e aggiornamento a tutti i livelli, definire regole (policy) chiare e condivise specifiche per l'utilizzo dei Social Media e controllare e misurare il loro livello di adozione e la loro efficacia nel tempo rispetto all'evoluzione delle minacce.

Inoltre è fondamentale responsabilizzare gli utenti e le strutture aziendali coinvolte, a qualsiasi titolo, dall'uso dei Social Media, adottare le tecnologie necessarie, moderare la conversazione social per prevenire gli incidenti (in real time!) e creare processi e team multidisciplinari in grado di gestire le crisi.

028941

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.