Comment mettre en place une veille sur l'e-réputation de votre entreprise ? (1ère partie)

Domaine :	**Recherche**	Référencement
Niveau :	**Pour tous**	Avancé

Les exemples commencent à se multiplier d'entreprises ayant eu à pâtir d'une mauvaise e-réputation suite à des actions d'internautes sur YouTube, Facebook ou autres sites web communautaires ou non. Pour une société, il convient de plus en plus d'être réactive sur la façon dont on parle d'elle en ligne. Une veille sur cette e-réputation est donc essentielle et de plus en plus d'acteurs se positionnent sur ce marché. Dans cet aticle en trois parties, nous allons esssayer de faire un tour complet de cette thématique et de voir comment mettre en place en interne de l'entreprise ce type de veille...

Que dit-on de vous sur le web ? De vos produits ? De vos services ? Des campagnes publicitaires que vous menez ?

Avec l'avènement de réseaux sociaux comme Facebook ou Twitter, qui permettent une conversation mondiale et en temps quasi-réel de tous avec tous, il est fort possible que l'on parle de vous « dans votre dos virtuel » et la réputation de votre entreprise peut être mise à mal en quelques heures. Les cas ne manquent d'ailleurs pas depuis quelques années. Trois exemples parmi d'autres :

- En 2004, une vidéo postée sur Youtube montre comment il est possible d'ouvrir un cadenas de la marque Kryptonite avec un stylo Bic en quelques secondes. 3 jours après sa mise en ligne, 1,5 millions de personnes l'ont visionnée. La société accepte d'échanger les produits défectueux. Coût de l'opération : 10 millions de dollars. « L'affaire Kryptonite » a été le révélateur des risques encourus par les marques sur le web.

- Durant l'été 2007 en Angleterre, la banque HSBC décide de profiter des vacances scolaires pour augmenter les intérêts des prêts étudiants. Un groupe créé sur Facebook par le principal syndicat étudiant amène la société à faire marche arrière.

- En septembre 2008 le cours de bourse d'United Airlines s'effondre de 75% suite à la fausse annonce de sa liquidation judiciaire relayée par Google News.

Si ces sociétés avaient mené une « veille image » en temps réel, il y a fort à parier qu'elles auraient pu juguler la crise bien plus rapidement qu'elles ne l'ont fait. Il devient donc de plus en plus nécessaire de surveiller et de gérer son e-réputation...

Ce concept a emergé en 2009, mais ce marché va exploser dans les 3 ans à venir. Le blog spécialisé Cadderéputation (http://caddereputation.over-blog.com) qui recensait une vingtaine de sociétés sur ce créneau en décembre 2008 en compte déjà 93 quelques 9 mois plus tard ! Il n'y aura pas de place pour tout le monde...

Mais que recouvre exactement le terme d'e-réputation? Notre définition est la suivante :
L'e-réputation d'une organisation est composée des données explicites et implicites, diffusées sur le web à la fois par l'organisation elle-même, ses employés, ses clients, ses concurrents ainsi que par des personnes-relais qui ne sont ni les uns, ni les autres (bloggeurs, twitterrers,...).

Concrètement l'e-réputation est générée par :

Ce que l'organisation dit d'elle-même explicitement :
- actions de communications corporate, communiqués de presse
- interviews de ses dirigeants, cadres,...

Ce qu'elle dit d'elle implicitement :
- actes qui peuvent être traçables : ex : modification tendancieuses de la page la concernant sur la Wikipedia, détectables via Wikiscanner (http://wikiscanner.virgil.gr/).

Ce que ses employés disent d'elle explicitement mais généralement de manière anonyme :
- exemple : les sites de notation d'entreprise (notetonentreprise.com).

Ce que ses employés disent d'elle implicitement :
- ex : données professionnelles mises en ligne sur LinkedIn ou Viadeo (fonction dans l'organisation, thème de travail, discussions entre employés via un forum) qui, une fois agrégées, peuvent fournir d'intéressantes informations.

Ce que ses clients disent d'elle explicitement :
- ex : blogs d'utilisateurs d'un produit, forums de discussion (http://www.ciao.com/).

Ce qu'ils en disent implicitement :
- systèmes de notation d'entreprise autour de thèmes éthiques comme l'empreinte écologique ou le travail des enfants (http://www.transnationale.org/).

Ce que ses concurrents disent d'elles explicitement :
- publicités comparatives, interviews comportant des attaques de produits concurrents.

Ce qu'ils disent de manière anonyme :
- Attaques dans des forums de discussion, création de vrais-faux blogs et tout ce qui s'apparente à des actions de déstabilisation par l'information.

Ce que des personnes-relais qui ne sont aucune des entités déjà identifiées en disent :
- Bloggeurs qui relaient une information
- Utilisateurs de Twitter, Facebook,...

Comme on le voit, les champs à surveiller sont nombreux et cela nécessite la mise en place d'une veille à large spectre. Il est évidemment possible de l'externaliser en passant par l'une des 93 sociétés évoquées ci-dessus (sans doute 95 depuis la rédaction de ce billet :-). Certaines ont développé leur propre solution logicielle et d'autres utilisent des logiciels spécifiques (Digimind e-réputation, AMI opinion tracker, Cymfony Maestro) pour les mettre au service de leurs clients.

Le coût de ces solutions va de quelques dizaines d'euros par mois à quelques centaines et se lancer dans un benchmark peut être rapidement chronophage tant elles sont nombreuses et disposent de leurs propres spécificités (type de sources prises en compte, serveur ou Saas, types de rendus graphiques,...).

Si l'on n'a pas de budget pour cela et/ou que l'on souhaite maîtriser le système de bout en bout, il est toutefois envisageable de réaliser sa veille en interne. La puissance du RSS et le nombre de sites web et services qui l'utilisent permet en effet de mettre en place facilement toutes sortes de veille sur internet sans avoir à rougir de la qualité des résultats obtenus.

Mise en garde

Avant de se lancer, il faut toutefois être conscient des inconvénients liés à ce choix :
- Nécessité de mener une veille sur les nouveaux outils à intégrer dans sa veille e-réputation.
- Nécessité d'un suivi quasi-permanent de ce qui se dit de vous afin d'être en mesure de contre-attaquer si nécessaire.
- Création de tableaux de bords et graphiques à réaliser manuellement.

Il ressort de ces trois éléments que la veille e-réputation est chronophage et nécessite une grande disponibilité de la part de ceux qui la pratiquent. Le risque étant que la gratuité des outils soit compensée négativement par les coûts humains de celle-ci, raison pour laquelle

chaque organisation doit avant en évaluer sérieusement la faisabilité avant de se lancer dans l'aventure. Si vous êtes partant, les choses commencent maintenant.

1ère étape : Choisir les mots-clés que vous souhaitez surveiller.

A l'instar de toute démarche de veille, la première étape consiste à déterminer les mots-clés que vous allez mettre sous surveillance. Cette démarche est toutefois simplifiée ici car il s'agit de termes clairs et déjà identifiés. Pas de synonymes à gérer donc, mais des risques de pollution quasiment impossibles à gérer si votre société s'appelle Dupont ou ... Total.
Afin d'être le plus concret possible nous utiliserons durant cette série d'articles la « société » Outils Froids. On peut donc choisir de mener sa veille sur les éléments suivants :

- Nom de l'organisation : « Outils Froids »
- URL du site corporate : http://www.outilsfroids.net/
- Noms de principaux dirigeants et des personnes de l'entreprise susceptibles de s'exprimer ou d'être citées : « christophe deschamps »
- Noms des marques (produits, services) proposées par la société : ouvrage « Le nouveau management de l'information ».
- Sites web spécifiques consacrés à ces marques.

2ème étape : Faire une liste exhaustive des sites et services que vous allez devoir mettre sous surveillance

- Médias : qu'il s'agisse de médias classiques (TV, radio, presse papier) utilisant le web pour diffuser de l'information sur le web, de « pure-players » internet (ex : Le Journal du Net) ou de plateformes de journalisme citoyen (Agoravox).
- Les forums et les listes de discussion : moins centrales qu'il y a quelques années car concurrencées par les sites à contenu social mais toujours très actives et donc indispensables à mettre sous surveillance.
- Les blogs et leurs commentaires : parce qu'ils sont devenus d'incontournables relais d'information et peuvent vite se transformer en « caisses de résonnance ».
- Les sites d'avis de consommateurs : ils permettent d'avoir des remontées clients directes mais aussi de surveiller d'éventuelles attaques de concurrents sur ces mêmes sites.
- La wikipedia et autres encyclopédies collaboratives : si votre société dispose d'une page sur ces sites, vous devez être en mesure de suivre l'évolution de celles-ci puisqu'elles sont éditables par tous.
- Les sites de « social networking » professionnels : les services de types LinkedIn ou Viadeo, qui permettent initialement de générer des contacts professionnels, disposent de leurs propres forums de discussion qu'il sera nécessaire de surveiller au même titre que les forums de Yahoo ! Groupes. Il peut également s'avérer utile de vérifier que vos employés inscrits sur ces services n'en disent pas trop long sur leurs activités au sein de la société. Ces sites font en effet le régal des hackers qui y pratiquent le « social engineering *».
- Les services de micro-blogging : Facebook (statuts) et encore plus Twitter sont devenus des caisses de résonnance à l'échelle planétaire. L'information peut y circuler à grande vitesse et avoir des conséquences désastreuses (cf. le cas Motrin en février 2009 - http://fr.readwriteweb.com/2008/12/04/analyse/media-sociaux-et-marques-retour-dexperience-sur-le-cas-motrin/).

En partant de cette base, nous verrons le mois prochain quels sont les outils et services gratuits que l'on peut articuler pour surveiller l'ensemble de ces sources.

** Pratiques basées sur l'imposture, le culot, l'abus de confiance, etc., ayant pour but d'exploiter l'aspect humain et social de la structure auquel est lié le système informatique afin de l'infiltrer (ex. se faire passer pour un technicien chargé de sécuriser le système informatique auprès d'un employé afin de récupérer ses mots de passe).*

Christophe Deschamps
Consultant et formateur en gestion de l'information.

Responsable du blog Outils Froids (http://www.outilsfroids.net/)

Réagissez à cet article sur le blog des abonnés d'Abondance :
http://abonnes.abondance.com/blogpro/2009/09/comment-mettre-en-place-une-veille-sur.html