

Management des noms de domaine :

Comment protéger et valoriser sa marque

L'importance que peuvent accorder les entreprises à une stratégie globale de gestion de leurs noms de domaine (ND) n'est jamais assez grande. Sous l'effet de la mondialisation, le marché s'est internationalisé, laissant place à une position grandissante de l'Internet. Il a, de ce fait, fragilisé les sociétés en mettant leurs noms de domaine à la merci du piratage. Les entreprises sont donc contraintes à enregistrer des centaines de ND pour éviter que leur activité ne soit interrompue et que leur marque ne soit exploitée par des cybersquatteurs. Les préjudices causés par les cybercriminels à la réputation des entreprises et la perte de revenus qui en découle ont été recensés dans le monde entier.

Afin de définir les mesures à prendre pour éviter que l'entreprise, son produit ou ses services ne subissent ces préjudices, il est bon qu'elle ait une parfaite compréhension de la nature du risque qu'elle encourt. L'entreprise devrait alors *s'informer des meilleures pratiques en matière de gestion de noms de domaine* et procéder à une *évaluation de son système de gestion en cours*. Enfin, une entreprise devrait être consciente de *l'expertise et des ressources dont elle dispose pour gérer de manière efficace et proactive son portefeuille de ND*. Si cela n'est pas le cas, l'entreprise doit alors faire appel aux services d'une société spécialisée en gestion et protection de portefeuille de ND.

LES MENACES : DES PREJUDICES CAUSES A LA REPUTATION
D'UNE SOCIETE A LA PERTE DE REVENUS

L'Internet Corporation for Assigned Names and Numbers (ICANN) est une organisation internationale à but non lucratif, dont la mission est de réguler l'enregistrement des noms de domaine et de surveiller les abus de noms de domaine. L'ampleur et la gravité de la menace qu'encourt une entreprise sont décrites dans un rapport établi en 2006 par le Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC) :

« Le piratage des noms de domaine peut perturber ou gravement nuire aux opérations commerciales d'un registrant (entreprise), notamment par la [...] dénégation et le vol de ses services de messagerie électronique, la divulgation non autorisée de ses informations par hameçonnage de sites web et l'inspection de son trafic Internet (écoute électronique). Enfin, la dégradation du site web du registrant peut également causer des torts à sa réputation et à sa marque. »

Ces menaces sont rendues possibles par la vulnérabilité du système d'enregistrement du ND. Le système de nom de domaine (DNS– Domain Name System) fonctionne comme un annuaire téléphonique automatisé, à la différence qu'il remplace les adresses numériques du protocole Internet (IP) par un seul nom (généralement le nom de la marque). Les **registrars** ont besoin de l'ensemble des coordonnées des **registrants** (« propriétaire » du ND) pour fournir l'enregistrement. Ces coordonnées sont ensuite rendues accessibles au public sur Internet grâce à un service appelé Whois. Chaque extension de nom de domaine de premier niveau ou TLD (top-level domain) (.com ou .fr par exemple) a un **registre** responsable de la gestion des noms de domaine et de leur réglementation. Le registrant est responsable de la mise à jour des informations qui figurent dans le Whois. Dans le cas où le registrant oublie de renouveler un nom de domaine, celui-ci peut se voir racheté par un tiers malintentionné, potentiellement dangereux pour la société ou le produit.

La récente commercialisation de nouveaux ND de premier niveau a augmenté les chances de la marque d'une société d'être piratée par un cybersquatteur qui : (1) acquiert les noms de domaine d'une société dont les données ont expiré et essaie de revendre le nom à un prix élevé ; (2) enregistre la marque d'une société sous une extension différente en redirigeant les clients sur un site contrefait ; et (3) enregistre des noms de domaine identiques à celui de la société mais dont seule une lettre est altérée (on appelle cela le typosquatting).

McAfee, l'entreprise américaine de logiciel anti-virus, a répertorié 1,9 million de variantes des 2771 noms de domaines les plus prisés et a constaté qu'un client ordinaire qui épelle mal une adresse Internet connue a une chance sur quatorze de tomber sur un site typosquatté ([What's In A Name: The State of Typo-Squatting 2007](#)). Le cybercriminel redirige le trafic Internet vers un site contrefait, et détourne toute l'activité de la société en mettant potentiellement le consommateur en danger de vol d'identité et en lui donnant accès à des informations illégales sur une entreprise ([US Government Accounting Office rapport 2005](#) ; ICANN).

Le conseiller d'entreprise pour les marques de la société pharmaceutique Pfizer a déclaré dans une interview : « *Je pense que toute altération de votre marque dans un nom de domaine pouvant prêter à confusion est une violation qui fait perdre de l'envergure à votre marque et qui, si l'on n'y prend garde, peut porter atteinte à vos revenus et à votre capital marque.* » ([The Register](#), août, 2007). Selon l'étude indépendante menée par Mazerov Research and Consulting (une société commerciale américaine), « *une interruption importante de l'activité a des effets durables sur l'entreprise après environ 88 minutes. Autrement dit, en moins d'une heure et demi, les dommages causés à l'entreprise auront des conséquences sur le long terme.* »

DE RECENTES DECOUVERTES ANNONCENT UN ACCROISSEMENT
DES RISQUES

- Parmi tous les noms de domaine enregistrés, au moins 8,65% le sont avec des informations Whois erronées ou incomplètes. Cette pratique facilite la tâche des cybersquatteurs. ([US Government Accounting Office](#))
- EURid, le registre de noms de domaine .eu basé en Belgique a suspendu plus de 74 000 noms de domaine et a entamé des actions en justice contre 400 registrars pour avoir enregistré des noms dans l'intention de les revendre, ce qui est contraire à la loi régissant les contrats entre registrars et registres. ([The Register](#), 2007)
- Les cinq pays dont les sites seraient les plus vulnérables à la cyberintrusion sont : le Royaume-Uni (7,7%), le Portugal (6,5%), l'Espagne (5,9%), la France (5,4%) et l'Italie (4,1%). ([McAfee Report](#), 2006)
- Les cas de cyberintrusion enregistrés par l'Organisation Mondiale de la Propriété intellectuelle (OMPI) ont augmenté de 48% en 2005.

L'OMPI a noté quatre évolutions récentes dans le système d'enregistrement de ND qui ont augmenté les risques pour les entreprises, qu'elles soient petites ou grandes :

- l'enregistrement automatique de noms de domaine expirés et le placement sur des sites portails pay-per-click ;
- la possibilité d'enregistrer des noms de domaine gratuitement pour une durée de cinq jours de test ;
- la prolifération de nouveaux registrars ;
- et la disponibilité de nouveaux noms de domaine de premier niveau.

L'OMPI note que ces évolutions augmentent les possibilités pour un tiers malintentionné d'enregistrer des centaines de noms de domaine en très peu de temps, contrevenant ainsi aux droits de la propriété intellectuelle. Depuis l'année 2000, le nombre de registrars a énormément augmenté, ce qui pour l'OMPI « *est d'autant plus inquiétant que, dans certains cas, les registrars semblent s'associer ou participer à des pratiques de cyberintrusion.* »

LES COMPLICATIONS : LES LOURDEURS ADMINISTRATIVES QU'IMPLIQUE LA GESTION DE PORTEFEUILLES DE ND

Surveiller les violations de la propriété intellectuelle et prendre des mesures préventives sont des tâches qui s'ajoutent aux lourdeurs administratives d'une société. Sans compter la tâche, en apparence simple, qui consiste à mettre à jour l'enregistrement du ND afin d'éviter qu'un pirate ne s'empare des noms de domaine de la société. La récente mise à disposition de noms de domaines de premier niveau (TLD) pousse les sociétés à revoir la manière dont ils gèrent leur portefeuille de noms de domaine.

Tout récemment (en juin 2008), l'ICANN a voté en faveur de l'ajout de tout TLD qui n'a pas plus de 64 caractères. Certaines sociétés de gestion de ND prévoient que les multinationales enregistreront encore plus de nouveaux ND pour faire face à la situation. De nos jours déjà, les entreprises disposent de très gros portefeuilles pour se prémunir contre les cybercriminels. La gestion de ces portefeuilles est devenue complexe. Selon l'ICANN, la complexité s'accroît à cause « *des circonstances changeantes (le type d'organisation, la politique mise en œuvre, l'économie, la langue, la culture, le cadre juridique et les relations avec le gouvernement) des différents codes de pays des TLD et des organismes qui les gèrent.* »

LES LITIGES : PROACTIF CONTRE REACTIF EST LE MEILLEUR
RETOUR SUR INVESTISSEMENT

Une société qui recherche des solutions juridiques au problème de la cyberintrusion rencontrera inévitablement des obstacles. Aux États-Unis, une loi protégeant les propriétaires de marques contre la cyberintrusion, Anti-Cybersquatting Consumer Protection Act (ACPA), a été votée. Toutefois, un cyberintrus qui ne réside pas sur le territoire des États-Unis échappe à cette loi. L'OMPI prévoit un service de résolution de litiges sur les marques des noms de domaine [Trademark Domain Name Dispute Resolution Service](#) et l'ICANN a instauré une politique homogène de résolution de litige concernant les noms de domaine [Uniform Domain-Name Dispute-Resolution Policy](#) :

« Tous les registrars dont les extensions des noms de domaine de premier niveau sont .biz, .com, .info, .name, .net et .org doivent suivre la politique homogène de résolution de litige concernant les noms de domaine (Uniform Domain Name Dispute Resolution Policy plus souvent appelée « UDRP »). Pour qu'il puisse invoquer cette politique, le propriétaire de la marque devra soit (a) déposer une plainte auprès d'une juridiction compétente contre le détenteur du nom de domaine (ou si cela est justifié, intenter une action in-rem concernant le nom de domaine) ou (b) dans le cas d'enregistrement abusif, déposer une plainte auprès d'un service agréé de résolutions de litiges. »

Il s'avère qu'appréhender un cybercriminel est coûteux, les frais judiciaires prennent beaucoup de temps et il est souvent vain de chercher à être dédommagé des pertes de revenus occasionnées. Les ressources devraient être davantage orientées vers la prévention que vers les règlements de conflits. Le fait est que les entreprises, actives notamment dans les domaines bancaires, de détaillants et de la pharmaceutique, sont en permanence les cibles de cyberintrus qui opèrent au niveau international. Un individu en Chine qui a récemment enregistré 10 000 noms de domaine a suscité la méfiance de la part d'un registre européen. Le registre a suspendu les enregistrements de

domaine de cette personne, en mettant en doute le bien fondé d'un si grand nombre de noms de domaine pour une seule personne. Sans une stratégie de gestion proactive, les entreprises qui disposent de gros portefeuilles de noms de domaine pourraient être mêlées à de fréquentes et longues querelles juridiques.

Une stratégie proactive permet de couper court à l'action du cybercriminel grâce à un système de veille efficace et un portefeuille complet de noms de domaine. Cependant le retour sur investissement du portefeuille d'une société est plus important que sa gestion. Le nom de domaine est un outil de marketing qui donne une valeur ajoutée à votre marque. De plus, il y a un avantage certain dans l'enregistrement de noms de domaine au niveau local. Les moteurs de recherche tels que Google ont tendance à classer le site web selon le TLD d'origine. Par exemple, un site web français .fr sera plus visible en France qu'un site .com en anglais. Cela est dû au fait que les consommateurs potentiels qui surfent sur le web filtrent les résultats sciemment pour n'en obtenir qu'au niveau local.

LES SEPT MEILLEURES PRATIQUES EN MATIERE DE GESTION DE PORTEFEUILLE DE NOMS DE DOMAINE

Considérez vos noms de domaines comme des biens d'entreprise

La gestion de votre portefeuille de nom de domaine fait elle partie de la stratégie globale de votre entreprise ? La gestion de votre portefeuille de noms de domaine est elle en adéquation avec les objectifs et missions de votre entreprise? Si la réponse est non, vous comprendrez pourquoi votre entreprise n'a pas considéré votre portefeuille de ND comme un bien d'entreprise important à protéger et à valoriser. Les risques sont trop importants pour ne pas développer une stratégie globale de gestion de noms de domaine. Et les occasions de valoriser ce bien sont trop nombreuses pour ne pas en tenir compte.

Gestion de nom de domaine centralisée

Choisissez un seul gestionnaire pour vos ND pour réduire les coûts, les risques et n'avoir qu'un seul point de contact (contact administratif de l'entreprise). Au fur et à mesure que de nouveaux noms de domaines de premier niveau deviennent disponibles et qu'une entreprise crée son e-commerce pour ses produits et ses services, son besoin d'acquérir continuellement de nouveaux noms de domaine peut lui faire oublier de tenir certaines échéances. Il est nécessaire de disposer d'un système de gestion efficace et d'une stratégie globale qui protège et optimise la valeur de vos marques.

Effectuer des audits systématiques de votre portefeuille de ND

Faites tout de suite des audits de tous vos noms de domaine. Est-ce que les dirigeants des différents services de votre entreprise qui gèrent les noms de domaine appliquent tous les mêmes politiques de mises à jour et de gestion ? Après un audit complet dans votre entreprise, vous devriez développer des procédures systématiques de renouvellement et d'acquisition de nouveaux noms de domaine.

L'audit et la centralisation de votre portefeuille de marque doivent être faits simultanément

Dans de nombreux pays, pour procéder à l'enregistrement d'un nom de domaine, on demande à ce qu'il soit associé également à une marque ou à une société locale. Voilà pourquoi il est recommandé d'effectuer un audit et la centralisation de votre portefeuille de marque au même moment où vous centralisez votre portefeuille de ND.

Surveiller les informations liées à l'enregistrement de votre nom de domaine pour que les mises à jour soient bien effectuées

Prenez des dispositions pour être sûr d'avoir les ressources et la technologie nécessaires qui garantiront la mise à jour de vos noms de domaine et assureront votre contrôle sur tout le processus. La mise à jour des données dans le Whois est primordiale pour éviter que les cyberintrus ne s'emparent de vos ND et ne vous les revendent à des prix exorbitants ou ne redirigent votre trafic Internet vers un site contrefait. Le renouvellement de vos ND pour une période plus longue qu'une année facilitera les tâches administratives.

Rester informé des nouvelles menaces

N'attendez pas que la crise (la contrefaçon, l'interruption de services, un accès non autorisé à la société et aux informations concernant vos consommateurs,...) face surface pour réagir. Consacrez du personnel à la surveillance des éventuelles menaces, afin qu'il puisse évaluer les dégâts possibles, développer un plan d'action et prendre les mesures nécessaires pour protéger votre portefeuille de ND.

Monétiser ses noms de domaine

L'utilisation marketing et commerciale des noms de domaine est un élément capital de la valorisation de la marque ; Une bonne utilisation d'un portefeuille de noms de domaine peut faire économiser plusieurs milliers d'euros en achat publicitaire, ce qui compense largement les coûts d'achat et de gestion.



EXTERNALISEZ LA GESTION DE VOTRE PORTEFEUILLE DE NOMS DE DOMAINE

L'externalisation de la gestion d'un portefeuille de noms de domaine consiste à faire appel à un spécialiste des noms de domaine pour gérer l'audit, le monitoring, la centralisation, les renouvellements et les récupérations de noms de domaine. L'objectif est de simplifier la gestion en bénéficiant d'un contact unique qui va gérer toute la partie administrative, technique et stratégique des ND.

Le résultat sera d'obtenir un ensemble de noms de domaine complet qui garantira l'avenir et la valeur de la marque. On sait maintenant qu'un portefeuille incomplet de noms de domaine conduit inévitablement à des risques qui dévaluent d'autant la marque correspondante.



3A boulevard du Prince Henri, L-1724 Luxembourg
tél. +352.20.20.31.21 fax. +352.26.44.18.43

contact: Nicolas VAN BEEK