INTERNET

Le racket numérique menace de plus en plus les entreprises

Si certaines entreprises tirent profit du web, bon nombre d'entre elles subissent encore les effets pervers du média. Toute entreprise présente sur la Toile est sujette à des malversations dont les conséquences peuvent être désastreuses.

FLAVIO QUARANTA
Associé,
IC Agency
Genève.

DAVID SADIGH
Associé,
IC Agency
Genève.

LES RISQUES liés à internet ne se cantonnent pas, comme on le croit encore trop souvent, à la seule sécurité informatique. Plus globalement, c'est le patrimoine économique de l'entreprise qui est menacé: sa marque, ses produits, sa réputation et celle de ses dirigeants, ou même ses stratégies. Il y a une dizaine d'années dans le monde réel, les réputations se construisaient en plusieurs décennies. Les produits avaient du temps pour convaincre, les entreprises pouvaient tabler sur une connaissance approximative de la concurrence pour infléchir leurs stratégies.

Aujourd'hui sur internet, un produit est évalué le jour de sa sortie par des milliers de clients qui partagent leur opinion avec l'ensemble des clients potentiels. Une campagne de diffamation peut nuire à une marque comme jamais auparavant, et de façon foudroyante.

On assiste actuellement à une recrudescence d'actions «offensives» de plusieurs types, portant parfois gravement atteintes aux établissements qui en sont les victimes. Les répercussions sont graves: perte de clients dans un laps de temps très court, chute des ventes, manque de confiance durable envers un produit, une entreprise ou encore un dirigeant. La campagne de déstabilisation qui a visé l'industrie européenne du saumon d'élevage, avec les conséquences qu'on connaît, est une bonne équivalence pour jauger l'envergure du péril qui guette aujourd'hui des produits qui semblent «à l'épreuve des balles».

Les menaces sont complexes et évoluent sans cesse

Il ne se passe pas deux mois sans que de nouveaux risques apparaissent. Ils ne sont généralement pas le fruit du hasard, mais le résultat de phénomènes complexes, mis sur pied par des individus peu scrupuleux. Les exemples abondent. Certains datent des premiers temps du World Wide Web, comme le cybersquatting, d'autres ont fait leur apparition tout récemment dans la panoplie des racketteurs, comme le phishing.

Le cybersquatting, c'est l'utilisation abusive de noms de domaine qui, selon toute vraisemblance, devraient appartenir au capital marque de l'entreprise (exemple: jeboycotte danone.com ou banquecantonaledegeneve.net). Contrairement aux idées reçues, le phénomène n'est pas mort: plus de 300 grandes entreprises suisses possèdent des noms de domaine détenus, souvent illégalement, par des personnes étrangères à l'entreprise. Le cybersquatting représente un risque important à plusieurs niveaux, notamment en termes de tort à l'image de marque.

Des solutions permettent toutefois de protéger son capital marque sur internet, et d'être averti lorsque ces réservations illicites ont lieu. Rares sont les entreprises conscientes de ce problème, et plus rares encore celles qui ont pris des mesures de protection.

Des attaques plus vicieuses peuvent être menées contre les entreprises. Le 31 mars dernier, plusieurs millions de clients de la Citibank ont reçu un mail «officiel» de leur banque, les invitant à entrer leur code secret pour accéder à une communication importante. Parmi eux, une proportion importante a obtempéré. Résultat: des dizaines de milliers de clefs secrètes se trouvent maintenant à la disposition d'inconnus aux intentions très peu philanthropiques. Ce phénomène, dénommé *phishing*, augmente de façon spectaculaire. Chaque jour, dix attaques majeures sont comptabilisées par l'Anti-Phishing Working Group.

DES DIZAINES DE MILLIERS DE CLEFS SECRÈTES SONT EN MAINS D'INCONNUS

Ce phénomène a déjà touché de nombreux établissements bancaires: Lloyds, HSBC ou encore Barclays pour ne citer que des établissements européens. La Suisse n'est de loin pas épargnée. Début avril, une attaque de phishing a fait sa première victime parmi les établissements helvétiques. Il s'agit de la Banque Cantonale Bâloise. Selon l'établissement, l'attaque était ciblée et visait des personnes habitant le canton. Comment les escrocs se sont-ils procurés les coordonnées de leurs futures victimes? Peut-être tout simplement en utilisant les fonctionnalités avancées d'un outil de recherche comme Yahoo!...

Internet peut servir à détourner la clientèle

En sus de ces attaques très particulières, le détournement même de la clientèle via les outils de recherche se fait de plus en plus courant. Chaque jour, 550 millions de recherches sont effectuées sur internet. Parmi celles-ci, de nombreuses recherches commerciales. Les internautes sont souvent dirigés, à leur insu, vers des sites parallèles à celui qu'ils pensaient consulter et offrant des produits similaires et affichant des publicités très ciblées, différentes en fonction notamment des pays. Comment demander à un client potentiel de faire la différence? Face à ces menaces en pleine effervescence, la plupart des entreprises ne sont pas à même de riposter. Pourquoi? D'une part, parce qu'internet ne se limite plus seulement au e-business, d'autre part parce que la palette des menaces va en s'élargissant, et enfin parce qu'il faut bien constater une méconnaissance généralisée à l'endroit des métiers de l'intelligence économique. Or l'enjeu est très souvent financier, car le «clic» se monnaie cher sur Internet. Pour rappel, le marché de la vente des mots-clés est estimé à 6 milliards de dollars pour 2006 («Golden Search», US Bancorp Pipper Jaffray, 2003).

Dès lors, il est primordial d'identifier la façon dont les publics de l'entreprise s'y prennent pour trouver la marque, les produits et services de cette dernière. «L'appel à une société spécialisée dans les problématiques de référencement s'avère alors une aide précieuse» précise Claude Baumann, directeur de la communication de l'Union Bancaire Privée.

Une discipline jeune et encore trop négligée

Bien anticipés, tous ces risques peuvent être court-circuités. Sur ce terrain, les entreprises gagnantes seront celles qui auront développé et aiguisé leurs facultés d'anticipation. Pour se prémunir contre de telles attaques, les compétences nécessaires sont multiples, et nécessitent souvent une collaboration interdisciplinaire (marketing/communication, informatique, juridique, voire R&D). Collaboration qui s'adjoint un ou plusieurs experts en intelligence économique, une discipline relativement jeune et encore trop négligée. ■

Les bénéfices immédiats du «cyberracketteur»

→ Gagner rapidement et à n'importe quel prix des parts de marché
→ Nuire durablement à une marque
→ Réduire la portée d'un avantage concurrentiel tangible (réputation de l'entreprise, satisfaction de ses clients)
→ Annuler ou réduire la portée d'une campagne de communication
→ Engendrer immédiatement des revenus en vendant la clientèle détournée (au travers de programmes comme AdSense de Google)
→ Influencer un choix, par exemple au niveau politique, lors d'une élection très serrée.

L'intelligence économique représente la meilleure défense contre les racketteurs

Il existe un point commun entre la clientèle visée par les banques, les marques de luxe, de l'automobile, ou les compagnies aériennes: leurs clients consacrent toujours plus de temps à internet.

Ils utilisent le web pour obtenir un renseignement spécifique, comparer les prix, identifier les points de vente les plus proches, ou encore connaître l'avis de personnes qui possèdent déjà le produit en question.

Or, malgré les alertes répétées des médias sur le manque de fiabilité d'internet en tant que source d'information, rares sont les utilisateurs qui mettent en doute les opinions de ces personnes.

Confrontation directe avec les racketteurs

On mesure le degré de nuisance qu'un individu ou une entreprise mal intentionnée peut exercer sur le produit d'un concurrent. Parmi les entreprises qui ont constitué en interne une cellule internet, bon nombre s'imaginent prêtes à faire face à toutes problématiques liées à leur présence en ligne. Or en s'ouvrant au monde, une entreprise s'expose à une confrontation directe avec des racketteurs avides de profits rapides.

Nous sommes très loin des hackers qui fouillent pour leur gloriole personnelle les numéros de comptes bancaires. La sécurité informatique ne peut rien contre les attaques pernicieuses des nouveaux corsaires du web. C'est là le terrain de chasse privilégié des experts en intelligence économique.

Contrairement à la veille, l'intelligence économique est une démarche proactive, orientée sur la prise de décision. Elle consiste à identifier et à surveiller le périmètre stratégique de l'entreprise, de manière à détecter rapidement les différents signaux émergents, et permettre aux responsables d'agir en toute connaissance de cause.

Les entreprises suisses sont encore rares à bénéficier de cellules dédiées. Lorsqu'elles en possèdent, le média internet est encore trop souvent laissé de côté.

Mise sur pied de solutions personnalisés

Pour Stéphane Koch, président de l'Internet Society Genève et spécialisé dans la criminalité économique, «la mise sur pied de solutions personnalisés visant à surveiller l'image de marque de l'entreprise permet d'accroître très sensiblement sa réactivité et de réduire les risques».

Sensibilisation, intégration d'internet dans l'ensemble de la stratégie d'entreprise, récupération et protection du territoire afférent à la marque et à ses dirigeants: les solutions existent. Reste à garder à l'esprit que si internet était un enfant, il n'aurait pas plus de 4 ans... et que c'est à cet âge-là que beaucoup de choses se jouent.