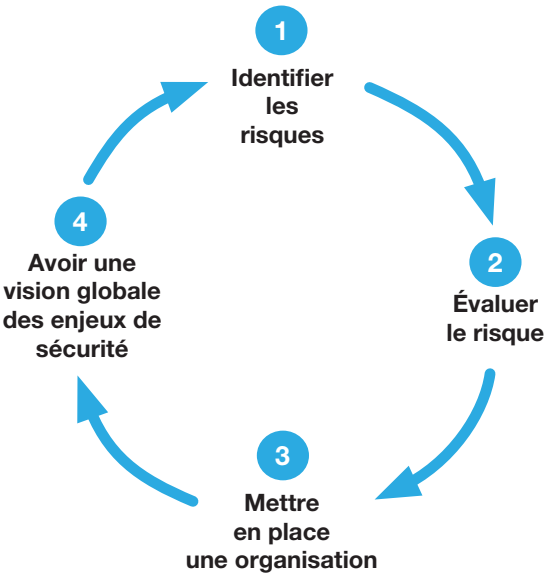
Dossier thématique n°9

Sécuriser
la gestion des noms de domaine

Ce dossier thématique s'adresse en priorité aux entreprises, dont la présence sur internet (sites commerciaux, campagnes de communication, adresses de messagerie électroniques…) dépend en partie de leurs noms de domaine et de la manière dont elles les gèrent. Pour autant, les risques associés à ces mêmes noms de domaine sont parfois mal connus. « Sécuriser » la gestion des noms de domaine, c'est en large partie avoir une vision des risques et des « bonnes pratiques » permettant de les limiter.

Appliquer les « bonnes pratiques » présentées ci-dessous renforce la protection de l'entreprise face à de possibles dysfonctionnements ou face à des attaques venant de l'extérieur. Les cas sont assez nombreux de noms de domaine « volés » (sex.com), transférés abusivement (ebay.de) ou suspendus pour faute de renouvellement (washpost.com).

Or ces problèmes peuvent être largement évités.



La démarche présentée dans ce dossier peut se résumer en quelques grandes étapes :

- identifier les risques « endogènes » et « exogènes » auxquels sont soumis les noms de domaine de l'entreprise et adopter les contre-mesures destinées à les limiter, sinon à les supprimer ;
- évaluer le risque lié à chaque nom de domaine (probabilité de réalisation / impact en cas de réalisation) et apporter un soin particulier à la protection des noms les plus stratégiques ;
- mettre en place une organisation, interne et avec les divers interlocuteurs extérieurs concernés, permettant de consolider de manière pérenne le dispositif de sécurisation ;
- avoir une vision globale des enjeux de sécurité et y intégrer la dimension noms de domaine au même titre que les autres.

Le niveau de complexité de cette démarche est directement fonction de la taille de l'entreprise. Les règles présentées sont très simples à appliquer sur ses noms de domaine par n'importe quelle TPE-PME.

Les entreprises détenant un grand nombre de noms de domaine, et dont les dispositifs de présence sur internet sont éclatés entre un grand nombre de partenaires et de prestataires, pourront naturellement gagner à faire appel à des spécialistes qui leur feront gagner du temps tout en leur apportant leur expérience de ces problématiques.

1 Identifier et évaluer les risques

Les risques liés à la gestion des noms de domaine sont de deux natures :

- Les risques « endogènes », qui se manifestent sous forme de dysfonctionnements et/ou de pertes de noms de domaine, en général conséquences de défaillances dans le dispositif de gestion mis en place ;
- Les risques « exogènes », qui se réalisent sous forme de vols ou de détournements de noms de domaine par des tiers exploitant une ou des failles dans le dispositif de gestion mis en place ;

Les risques endogènes

Cette catégorie de risques couvre tous ceux qui sont induits par le titulaire lui-même. On peut mentionner à titre d'exemple :

- Le non renouvellement d'un nom dans les délais, aboutissant à la suspension puis à la perte de celui-ci. Les noms hotmail.com et washpost.com ont été des cas célèbres. En général, la période de suspension suffit pour identifier le problème et induit un préjudice de quelques heures, parfois très coûteux. Mais dans le cas de noms moins utilisés, la négligence peut aller jusqu'à leur retombée dans le domaine public ;
- La non mise à jour de l'identité du titulaire d'un nom, aboutissant parfois à des situations d'une grande complexité juridique où il devient impossible d'établir clairement à qui appartient un nom, le titulaire ayant cessé d'exister. Des situations comparables peuvent survenir lorsque le nom de domaine d'une entreprise est déposé par l'un des associés en son nom personnel, et qu'il y a ensuite litige entre les associés. Les règles mises en place par l'ICANN indiquent par ailleurs clairement que des noms peuvent être supprimés si les données WHOIS ne sont pas correctes ;
- La « délégation » volontaire ou inconsciente de la titularité et/ou du contact administratif d'un nom de domaine à un prestataire ou à un partenaire, dont les intérêts peuvent un jour diverger de ceux de son client et qui pourrait être tenté d'utiliser contre lui le contrôle qu'il détient sur ses noms de domaine. Ce cas est extrêmement fréquent ;
- L'obsolescence des contacts et notamment des adresses de courrier électronique, induisant que le titulaire ne peut plus recevoir de messages liés à la gestion du nom de domaine. La conséquence immédiate de cette situation est que les demandes de modifications ne peuvent plus être approuvées ou rejetées, et que les rappels en cas de dépassement des délais de renouvellement ne seront jamais reçus ;
- L'abandon inconsidéré par le titulaire de noms de domaine servant de supports de courriels à des contacts administratifs d'autres noms du portefeuille, sans se douter qu'il ouvre ainsi une faille de sécurité dans son dispositif en permettant au tiers qui aura redéposé le nom de domaine de prendre le contrôle de tous les domaines dont les contacts continuent de dépendre du nom abandonné ;
- Une politique insuffisante (voir l'absence de politique) en matière de sécurisation de l'accès aux interfaces de gestion des noms de domaine. En général, les noms de domaine sont gérés et configurés via des interfaces web fournies par les bureaux d'enregistrement. Détenir le mot de passe permettant d'accéder à ces interfaces, c'est pouvoir repointer des noms, couper le service ou modifier les serveurs DNS et les contacts. Ce cas de figure est arrivé à twitter.com en 2009 ;
- Une organisation interne défectueuse ne permettant pas d'assurer la gestion des noms de domaine dans de bonnes conditions de sécurité. En règle générale, la gestion des noms est menée de manière empirique sans réflexion de fond sur les bonnes pratiques à respecter en terme d'organisation, ce qui crée des vulnérabilités en cas de dysfonctionnements (délais de résolution du problème) ou d'attaques (capacité moindre à identifier la nature de l'attaque et à y réagir de manière adéquate) ;

Les risques exogènes

Assez fortement médiatisés, les risques exogènes sont plus connus que les risques endogènes. Ils leur sont cependant intimement liés, car de nombreuses attaques de tiers sont rendues possibles, ou facilitées, par l'existence de failles dans les différents points évoqués ci-dessus.

- Le vol de noms de domaine est le risque le plus saillant, un certain nombre d'affaires ayant sensibilisé le public à cette éventualité. « sex.com » a été l'un des cas les plus célèbres de noms de domaine volés. Les motivations à ces vols sont multiples, depuis l'espoir de revendre le nom à des tiers, jusqu'à l'espionnage industriel (captation d'informations sensibles via les courriels) en passant par l'extorsion, la nuisance à l'image du titulaire ou l'interruption pure et simple du service ;
- Le dépôt immédiat par un tiers d'un nom de domaine sensible supprimé ou abandonné par erreur. Cette situation est fréquente, d'autant plus facilitée par l'existence d'outils automatiques et de systèmes permettant d'évaluer le trafic induit par un nom de domaine sur le point de retomber dans le domaine public. Les préjudices peuvent être considérables, depuis l'interruption des services web et courriel jusqu'au rachat en catastrophe du nom concerné à des prix largement supérieurs à ceux du marché ;
- Les transferts abusifs, permettant d'installer un nom de domaine sur des serveurs non « légitimes » une fois le nom transféré chez le nouveau bureau d'enregistrement, et de pointer ensuite le nom vers le site souhaité par l'agresseur. Des noms aussi célèbres que nike.com, ebay.de ou panix.com ont fait l'objet de ce type d'attaques ;
- Le détournement de noms de domaine au moyen de l'accès de l'agresseur à l'interface de gestion des noms de domaine concernés. Les cas de ce genre d'attaques sont moins bien connus, mais la presse s'est fait l'écho de litiges entre des entreprises et d'anciens salariés indélicats ayant utilisé leurs accès pour nuire à leur ex-employeur ;
- Des failles de sécurité dans les procédures d'échanges entre le titulaire et son prestataire, ou chez le prestataire lui-même. Ces risques peuvent se concrétiser si les accès ne sont pas sécurisés (https), ce qui permet potentiellement à des « hackers » de capter des informations. Autre exemple, le fait qu'il n'existe pas de système d'authentification / identification mutuelle des interlocuteurs peut favoriser l'usurpation d'identité du titulaire ou du prestataire par un tiers qui serait ainsi en mesure d'« exiger » des informations ou de « recommander » des actions portant préjudice au titulaire. Ce genre de mésaventure a déjà été subi par des titulaires dont les prestataires acceptaient les documents envoyés par fax en guise de justificatifs. Les agresseurs ont obtenu la mise à jour du contact administratif sur la base des seuls fax, et ont ensuite pu transférer les noms de domaine concernés ;

On préfèrera parler de « prestataire » au sens large, car il existe une grande variété d'acteurs pouvant intervenir dans la gestion des noms de domaine d'un client final, depuis le bureau d'enregistrement jusqu'aux employés de ce client en passant par des intermédiaires tels que des agences web, cabinets de conseils juridiques et autres.

Dans certains cas, c'est un partenaire commercial qui détiendra les noms de domaine ou en assurera la gestion. L'entreprise doit savoir évaluer le degré de fiabilité de ce partenaire et se protéger juridiquement contre toute surprise, par exemple via des contrats formels de concession d'utilisation des noms de domaine concernés, prévoyant leur « restitution » en cas de rupture des liens avec le partenaire.

La règle d'or en matière de sécurité étant que « la résistance d'une chaîne est égale à celle de son maillon le plus faible », un titulaire conscient des enjeux aura tendance soit à s'assurer que chaque maillon est « sécurisé » soit à raccourcir autant que possible la chaîne des intervenants, soit les deux. La situation idéale étant atteinte lorsque tous les noms d'un titulaire sont sous son contrôle juridique et administratif exclusif et direct, la partie technique restant généralement confiée à un prestataire.

L'évaluation des risques

Une démarche possible en terme d'évaluation des risques pourrait être :

- D'identifier le niveau de criticité de chaque nom de domaine du portefeuille (services associés, impact en cas de dysfonctionnement, suspension, perte, détournement ou vol…) ;
- D'analyser les données WHOIS en s'assurant que le nom est géré conformément aux bonnes pratiques décrites ci-dessous ;
- Pour les noms qui ne sont pas gérés conformément aux bonnes pratiques, d'évaluer la probabilité de réalisation du risque induit par ce non respect (par exemple, un nom servant de support de communication sur une marque phare aura plus de chances d'être attaqué qu'un nom défensif dans un TLD peu connu) ;
- De mettre en place un plan d'action pour corriger toute faille potentielle sur les noms stratégiques présentant de fortes probabilités d'attaques ou sur lesquels des dysfonctionnements entraîneraient des préjudices graves pour le titulaire ;
- De placer des outils de surveillance ad hoc sur les noms les plus stratégiques, notamment sur les données WHOIS et DNS relatives à ces noms ;

2 Limiter les risques endogènes

Nous allons aborder dans cette seconde partie les bonnes pratiques permettant de limiter les risques endogènes.

Maîtriser les renouvellements

Les dates d'échéance des noms de domaine doivent être connues et surveillées. Seules font foi les dates figurant dans les WHOIS officiels des registres en charge des TLD concernés. Il existe parfois des décalages entre les dates anniversaires de renouvellement des services chez un prestataire et les dates de renouvellement auprès du registre, ce qui est source d'erreurs.

Lorsque le prestataire propose ce service, la solution la plus sûre pour éviter des problèmes liés aux renouvellements est de basculer en mode « renouvellement automatique », le client conservant naturellement la capacité de demander formellement le non-renouvellement de tel ou tel nom. Cette pratique exige du client une mobilisation supérieure en terme de choix des noms à renouveler ou non (puisque le prestataire facturera automatiquement les noms à chaque échéance). Mais elle est aussi beaucoup plus sécurisante.

Le renouvellement pour X années permet de réduire le nombre d'échéances (1 seule fois tous les 5 ans au lieu de 5) mais ne résoud rien quant au fond, et limite la souplesse de gestion puisqu'obligeant le titulaire à avancer X annuités d'avance sur des noms qu'il voudra peut-être abandonner entre temps.

Lorsqu'un nom de domaine cesse brutalement de fonctionner, le statut en terme de renouvellement est la première chose à considérer.

Être réellement titulaire de ses noms de domaine

Tout comme l'entreprise est propriétaire des marques qu'elle détient, elle doit veiller à être titulaire (ou « registrant ») des noms de domaine qu'elle dépose ou fait déposer en son nom.

Il doit être formalisé clairement que l'entreprise est titulaire de tous les noms de domaine déposés dans le cadre de sa collaboration avec tel ou tel prestataire ou partenaire. Tout nom de domaine déposé par un tiers en relation avec l'entreprise devrait être restitué sans contrepartie supérieure aux frais occasionnés par l'opération, s'il a été déposé de bonne foi.

Cette règle est aussi valable dans le cas de noms de domaine déposés en leur nom par les associés d'une entreprise. Cette situation est souvent justifiée par la réalisation des dépôts avant que la personne morale ne soit créée. Mais une fois celle-ci dûment enregistrée, il est important que la titularité des noms de domaine lui soit transférée afin d'éviter que les titulaires « physiques » n'utilisent un jour cet avantage contre les autres associés.

Faire preuve de négligence sur cet aspect expose l'entreprise à des conflits autour de la possession et de l'exploitation du nom de domaine, si elle vient à se fâcher avec le prestataire ou le titulaire.

L'entreprise doit appliquer cette exigence à elle-même en veillant à ce que les noms qu'elle détient aient toujours pour titulaires des entités juridiques « actives » (maison-mère, filiales…). Des mises à jour sont donc nécessaires en cas d'évolution : fusions, cessions ou acquisitions, changement de raison sociale… Dans l'idéal, les titulaires des noms de domaine doivent être alignés sur les détenteurs des marques auxquels correspondent ces noms de domaine.

Les contacts : pertinents et pérennes

Les contacts, et notamment l'adresse de courriel du contact administratif, doivent être pertinents et pérennes. Il ne sert à rien d'inscrire en contact administratif le dirigeant de l'entreprise si celui-ci ne s'occupe pas du tout du dossier noms de domaine, même s'il est le seul représentant juridique de l'entreprise.

Par défaut, une adresse de courriel « générique » (dns.admin@exemple.fr) doit être utilisée afin d'éviter d'avoir à la mettre à jour à chaque changement de responsable du dossier. A contrario, en cas de départ du responsable, son adresse de messagerie électronique ne doit pas être supprimée. Dans l'idéal, elle doit être maintenue le temps que le nouveau responsable s'assure qu'elle n'est pas enregistrée en contact pour l'un des noms du portefeuille.

Dans une logique d'optimisation de la sécurité, il vaut mieux éviter que l'adresse de courriel de contact d'un nom de domaine ait ce même nom de domaine pour support. Ceci afin d'éviter les situations de blocage où un dysfonctionnement affectant le nom de domaine empêcherait aussi les messageries de fonctionner. En corollaire, il est impératif de ne pas abandonner un nom de domaine ayant servi de support de courriels avant de s'être assuré qu'il n'est effectivement plus utilisé dans les contacts.

Enfin, on peut aussi noter que les adresses de contact dépendant de comptes « gratuits » peuvent présenter des risques en terme de sécurité, si l'on se réfère à quelques affaires récentes. Quels que soient ses choix, l'entreprise doit veiller à conserver la maîtrise des adresses de contact aussi bien au niveau des noms de domaine que des codes permettant d'accéder aux messages ou d'en envoyer.

Les identifiants d'accès : keep your secret secret

Les identifiants et mots de passe permettant d'accéder aux interfaces de gestion des noms de domaine sont des données particulièrement sensibles. Toute personne les détenant peut se connecter au compte de n'importe quel endroit de la planète et effectuer toutes modifications sur les noms de domaine concernés : repointages, mises à jour des serveurs et des contacts ou transferts vers un autre bureau d'enregistrement.

Les identifiants et mots de passe ne doivent pas être communiqués par courriel ou notés sur des supports accessibles de tous. Ils doivent être confiés à un nombre volontairement limité de personnes bien identifiées et formellement habilitées à intervenir dans l'interface, le cas échéant en précisant les pouvoirs de chacun. Les codes d'accès doivent être suffisamment « robustes » et modifiés à intervalles réguliers. Tout départ de l'une des personnes de l'équipe doit automatiquement entraîner la mise à jour des mots de passe, cette règle étant aussi appliquée lorsque le portefeuille de l'entreprise est suivi spécifiquement par un ou des interlocuteurs au sein d'un prestataire, et que l'un de ces interlocuteurs vient à partir.

Dans la même logique de contrôle de la titularité des noms de domaine et des contacts administratifs, il est important que l'entreprise possède les « clefs » de l'interface de gestion de ses noms de domaine et soit la seule à les posséder. Cette question peut s'avérer délicate à gérer lorsqu'elle passe par un intermédiaire qui gère tous les noms de ses clients sur un même compte chez un bureau d'enregistrement donné. Quoique fréquente, cette situation n'est pas recommandée du point de vue de la sécurisation de la gestion des noms car elle induit une trop forte dépendance vis-à-vis d'un tiers. Un prestataire détenant un « co-accès » à l'interface peut faire ce qu'il veut avec les noms de l'entreprise, y compris modifier le mot de passe d'accès à l'interface à l'insu de son client en cas de conflit avec lui. Faute de mieux, le contrat encadrant la collaboration doit interdire toute pratique de ce genre.

Par mesure de sécurité, les codes d'accès aux interfaces doivent aussi être stockés dans un endroit sûr et accessible, en cas d'urgence et d'indisponibilité des personnes habilitées. Les personnes autorisées à obtenir les codes dans ces circonstances exceptionnelles doivent être identifiées et connues des bureaux d'enregistrement compétents, afin de pouvoir mener les actions nécessaires.

Une organisation interne adaptée aux besoins

Les trois principes en matière d'organisation interne sont :

- D'avoir un référent identifié sur le dossier, jouant le rôle « d'expert » maison et de coordinateur. Les pouvoirs de ce référent peuvent être très étendus dans le cas de mode de gestion concentrés, ou au contraire très limités dans le cas de gestions déconcentrées. Mais il doit y en avoir un dans tous les cas, afin de pouvoir gérer le second principe ;
- D'adopter une approche transversale associant les différentes compétences nécessaires, afin de pouvoir prendre des décisions en ayant une vision globale des besoins et des risques. Le vol d'un nom de domaine par exemple peut avoir des incidences en terme de chiffres d'affaire, d'image, de sécurité et de contentieux. Toutes les disciplines nécessaires doivent être associées au pilotage du dossier ;
- De disposer de procédures claires pour toute demande d'opération sur un nom de domaine de l'entreprise. Les procédures peuvent varier assez largement selon les modes de gestion adoptés, mais elles doivent permettre de savoir qui a fait quoi et dans l'idéal pourquoi. Cela permet de retrouver rapidement l'auteur ou l'initiateur d'une opération problématique et de comprendre ce qui a pu se produire. À l'inverse, toute demande d'opération ne respectant pas la procédure peut être identifiée comme suspecte, ce qui réduit d'autant les risques d'attaques dites « sociales » ;

L'objectif bien compris de l'organisation interne est de pouvoir limiter les risques tout en réagissant rapidement et avec pertinence aux dysfonctionnements comme aux attaques. Ceci nécessite à la fois compétence(s) et coordination. Le dossier thématique de l'Afnic consacré au Slamming insiste par exemple sur la valeur ajoutée d'un référent interne sensibilisé à ces pratiques frauduleuses et pouvant avertir ses correspondants en cas d'alerte.

3 Limiter les risques exogènes

Nous allons aborder dans cette troisième partie les bonnes pratiques permettant de limiter les risques exogènes.

Des échanges sécurisés entre titulaire et prestataire

La plupart des bureaux d'enregistrement proposent à leurs clients des interfaces de gestion permettant de gérer les noms de domaine sans passer par l'équipe du prestataire. Au-delà des mots de passe évoqués précédemment, il convient de s'assurer que l'accès se fait en mode https.

Cette solution est cependant rarement possible lorsque le titulaire passe par les services d'un revendeur (agence web, conseil…) gérant les noms de domaine de ses clients à partir de son propre compte chez un bureau d'enregistrement. Dans ce contexte, il sera nécessaire pour le client final de mettre en place avec son prestataire un système de communications limitant les risques d'attaques « sociales » :

- Identification claire des adresses de courrier électroniques utilisées par le client final comme par le prestataire. Tout courriel reçu d'une autre adresse portant sur la gestion des noms de domaine doit être considéré avec suspicion (mais pas nécessairement ignoré). Cette règle – qui n'exclut pas un regard critique porté sur les courriels apparemment « légitimes » - s'applique aussi aux courriers « papier » émanant d'un autre prestataire que celui avec lequel le client final est en contact ;
- Dans le cas de prestataires proposant à leurs clients des services d'accompagnement, identification claire des chargés de compte et des interlocuteurs habilités à intervenir sur les noms de domaine du client et réciproquement, des personnes chez le client habilitées à donner des instructions au prestataire ;
- Procédure de confirmation par un autre canal en cas d'opérations pouvant affecter la gestion du nom de domaine (pointage, modifications de contacts…). Cette dimension est parfois « transparente » pour le client final lorsque le prestataire prend tout à sa charge, mais nous nous trouvons alors dans le cas où le client ne contrôle rien, ce qui n'est pas souhaitable ;
- Confirmation de réception par le prestataire de toute demande d'opération menée sur les noms de domaine. Le client sait ainsi que ses instructions ont été prises en compte et menées à bien, et peut réagir s'il n'est pas à l'origine de ces demandes ;
- Existence d'une procédure et de contacts « d'urgence » permettant au client final d'obtenir une assistance immédiate de son prestataire en cas de problème grave (vol, suppression inopinée d'un nom…) ;

Bien que ce ne soit pas une condition absolue du choix d'un bureau d'enregistrement, le fait de passer par un prestataire ayant les mêmes heures ouvrables et capable de communiquer dans la langue du client peuvent être des atouts non négligeables dans les situations de crise.

Des niveaux de sécurisation adaptés à la criticité des noms de domaine

Tous les noms de domaine d'un portefeuille n'ont pas toujours besoin d'être surprotégés. Mais un bureau d'enregistrement qui n'offrirait pas la possibilité de bien sécuriser les noms de domaine qui lui sont confiés pourrait devenir source de vulnérabilités dans le dispositif global de sécurité de l'entreprise.

- Existence de systèmes de « restauration » permettant le retour immédiat à la configuration ayant précédé la modification jugée préjudiciable ;
- Possibilité de « verrouillage » des noms au niveau du bureau d'enregistrement. Les noms de domaine doivent être protégés contre toute opération non initiée par le titulaire. Le statut habituel dans les gTLDs est « RegistarLock » ou clientTransfertProhibited, clientUpdateProhibited, clientDeleteProhibited qui interdisent les transferts, modifications de données ou suppressions par des tiers ;
- Cette mesure de sécurité indispensable doit impérativement être complétée par la possibilité offerte au client final d'accéder via l'interface aux authInfo et autres codes permettant de déverrouiller les noms de domaine, et ceci sans l'intervention du bureau d'enregistrement. Dans le cas contraire, le client dépend de l'efficacité et/ou de la bonne volonté de son prestataire, ce qui arrive notamment dans le contexte où des intermédiaires sont les seuls à avoir accès à l'interface de gestion ;
- Mise en place de système de récupération automatique des noms stratégiques en cas de retombée dans le domaine public. Un certain nombre d'outils existent sur le marché, gratuits tant que le nom de domaine surveillé n'a pas à être récupéré. Ce niveau de sécurité est rarement mis en place aujourd'hui, mais il peut constituer une parade efficace à une suppression inattendue du nom de domaine du fait d'une attaque d'un tiers ayant par exemple réussi à « leurrer » le prestataire ou à accéder à l'interface de gestion ;
- Recours, pour les noms le plus stratégiques, aux services de « Registry Lock » c'est-à-dire au verrouillage des noms de domaine au niveau du registre du TLD, lorsque celui-ci propose cette possibilité ;

Des précautions internes prises par l'entreprise

Ces « précautions » sont de divers ordres et c'est la raison pour laquelle elles sont regroupées dans une partie spécifique. On peut mentionner :

- La prise en compte de la dimension noms de domaine dans la politique globale de gestion des risques de l'entreprise. Cette précaution peut avoir l'intérêt de compléter utilement cette politique tout en faisant comprendre pourquoi les enjeux liés à la gestion de noms de domaine ne doivent pas être négligés ;
- L'élaboration d'un plan de continuité d'activité en cas d'incident sur un nom de domaine stratégique, ce plan détaillant notamment les interactions avec le ou les prestataires concernés. Les intervenants sur le dossier doivent être formés et régulièrement entraînés à la mise en œuvre de ce plan ;
- La couverture par les contrats d'assurance des dommages potentiels liés à des incidents sur les noms de domaine. Cette dimension est encore peu développée en France, mais semble être devenue une évidence aux États-Unis ;
- La mise en place de surveillances sur les WHOIS afin de vérifier notamment que les noms sont bien verrouillés et que les informations enregistrées n'ont pas été modifiées à l'insu de l'entreprise ;

4 Pour aller plus loin

Les quelques liens proposés ci-dessous font référence à des cas réels de vols ou d'incidents sur des noms de domaine liés au non respect des règles exposées dans le présent dossier thématique. Nous avons aussi mentionné des articles et des documents traitant du même sujet.

Cas réels

Internal Twitter Credentials Used in DNS Hack, Redirect
http://www.wired.com/threatlevel/2009/12/twitter-hacked-redirected/

Firm to sue employee for domain name theft
http://www.out-law.com/page-4964

Washington Post Misses Domain Deadline
http://www.internetnews.com/xSP/article.php/3309801/Washington+Post+Misses+Domain+Deadline.htm

Grand Jury Indicts Daniel Goncalves On Domain Theft Charges
http://www.domainnamenews.com/legal-issues/grand-jury-indicts-daniel-goncalves-domain-theft-charges/6613

Major Domain Hijacking Alert: Industry Pioneer Warren Weitzman Has Over a Dozen Domains Stolen From his Enom Account
http://www.dnjournal.com/archive/lowdown/2009/dailyposts/20090721.htm

Hushmail DNS Attack Blamed on Network Solutions
http://www.eweek.com/c/a/Security/Hushmail-DNS-Attack-Blamed-on-Network-Solutions/

ISP Panix Domain Name Hijacked
http://www.thewhir.com/web-hosting-news/isp-panix-domain-name-hijacked

Articles et rapports

How To Protect Yourself Against Domain Name Hijackers
http://securityskeptic.typepad.com/the-security-skeptic/how-to-protect-yourself-against-domain-name-hijackers-.html

Vol de nom de domaine : comment l'éviter et que faire si ça vous arrive
http://www.olivier-duffez.fr/conseils-contre-vol-de-nom-de-domaine

How Secure Is Your Domain Name?
http://www.inc.com/articles/2001/06/23147.html

SPECIAL REPORT: How to protect your domain name from hijackers, porn pirates, and your registrar.
http://www.betterwhois.com/domainhijacking.htm

Protecting Your Domain Name: Control is the Key.
http://tcattorney.typepad.com/anticybersquatting_consum/2007/08/protecting-your.html

Rapport du SSAC – hijacking – 12 07 05
http://www.icann.org/announcements/hijacking-report-12jul05.pdf

Rapport du SSAC – SAC 044 - A Registrant's Guide to Protecting Domain Name Registration Accounts
http://www.icann.org/en/groups/ssac/documents/sac-044-en.pdf

L'Afnic est le registre des noms de domaine .fr (France), .re (Île de la Réunion), .yt (Mayotte), .wf (Wallis et Futuna), .tf (Terres Australes et Antarctiques), .pm (Saint-Pierre et Miquelon).

L'Afnic se positionne également comme fournisseurs de solutions techniques et de services de registre. L'Afnic - Association Française pour le Nommage Internet en Coopération - est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.

www.afnic.fr

Retrouvez tous les dossiers thématiques de l'Afnic :
http://www.afnic.fr/fr/ressources/publications/dossiers-thematiques-4.html