Les ordinateurs de Sony Pictures piratés, et paralysés

Les ordinateurs de Sony Pictures piratés, et paralysés

Décidement, Sony Pictures est une cible de prédilection pour les pirates. En 2011, c'est le site du studio qui avait été compromis et des données personnelles dérobées. A présent, c'est le réseau informatique qui a fait l'objet d'une intrusion.

Comme le rapporte The Verge, les salariés des différents bureaux de Sony Pictures ont ainsi découvert une image inattendue sur l'écran de leur ordinateur au moment de se connecter à leur session.

Une entreprise paralysée
Une image représentant un squelette écarlate les informait qu'ils avaient été hacké par #GOP. Le message précise que des données sensibles de l'entreprise et ont été dérobées. Les pirates menacent d'ailleurs de les dévoiler sur Internet si leur demande n'est pas satisfaite – une ou des exigences qui ne sont pas précisées.

Les salariés de Sony Pictures étaient hier encore dans l'incapacité d'utiliser les outils informatiques, d'envoyer par exemple un mail ou même de répondre au téléphone – vraisemblablement de la ToIP.
Outre le blocage des ordinateurs de Sony Pictures, ce sont des douzaines de comptes Twitter de Sony qui ont été provisoirement piratés afin de tweeter le même message sur le réseau social. L'entreprise a depuis repris le contrôle de ces comptes Twitter.
Une affaire de plus à suivre…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/les-ordinateurs-de-sony-pictures-pirates-et-paralyses-39810107.htm

---

Un virus informatique prend

pour cible la Russie et l’Arabie Saoudite

Un virus informatique prend pour cible la Russie et l’Arabie Saoudite

Un virus informatique très sophistiqué a lancé une attaque contre des opérateurs télécoms russes et saoudiens, a révélé la compagnie de cyber-sécurité Symantec.

Ce virus, baptisé « Regin », serait au moins aussi redoutable que « Stuxnet », qui avait causé de gros dégâts en 2010 dans le programme nucléaire iranien, retardant sans doute de plusieurs années les travaux des ingénieurs iraniens soupçonnés de mettre au point des armements nucléaires…
Stuxnet avait été développé par les services secrets américains et israéliens, selon des sources concordantes.

Un voleur qui fait disparaître ses traces…
Selon le ‘Financial Times’, qui cite lundi des sources au sein de Symantec, Regin pourrait lui aussi avoir été mis au point par des services secrets occidentaux, et serait d’une sophistication sans précédent… On ignore encore de quelle manière le virus infecte les systèmes informatiques, mais il s’est jusqu’à présent attaqué à des fournisseurs d’accès à internet en Russie, Arabie Saoudite, au Mexique en Irlande et en Iran.
Son objectif serait de dérober des données confidentielles, et il aurait la capacité de s’adapter à tous types de réseaux. Il serait aussi capable, dans certains cas, de faire disparaître toute trace de son passage une fois son forfait accompli… Regin aurait notamment ciblé les serveurs de messageries gérées par Microsoft, ainsi que les conversations de téléphones mobiles circulant sur de grands réseaux mondiaux.

L’industrie, nouvelle cible des « hackers », selon Kaspersky
Au même moment, Eugene Kaspersky, le directeur général d’une autre firme de sécurité informatique, Kaspersky Labs, a mis en garde contre la multiplication des cyberattaques contre les systèmes de groupes industriels, notamment dans le secteur énergétique (centrales électriques…). Selon lui, l’industrie est devenue la cible privilégiée du crime organisé, avec des attaques qui vont plus loin que les récents vols de données personnelles dont ont été victimes les clients de JP Morgan, Home Depot ou Target aux Etats-Unis. Les hackers ont notamment réussi à éviter que des chargements soient contrôlés dans des ports, ou à voler des stocks de céréales dans une usine ukrainienne en falsifiant les jauges pour qu’elles affichent des poids inférieurs à la réalité, a indiqué M. Kaspersky au ‘FT’…

L’an dernier, l’office de police criminelle intergouvernemental Europol avait rendu public le démantèlement d’un réseau de trafiquants de drogue, qui avaient « hacké » les ordinateurs du port belge d’Anvers… Les trafiquants étaient parvenus à déplacer les conteneurs contenant de la drogue pour leur éviter de subir des contrôles douaniers.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.boursier.com/actualites/economie/un-virus-informatique-prend-pour-cible-la-russie-et-l-arabie-saoudite-26186.html

Un livre consacré à la cybercriminalité souligne la nécessité d’un cadre juridique approprié

Un livre consacré à la cybercriminalité souligne la nécessité d’un cadre juridique approprié

Le magistrat sénégalais Pape Assane Touré a présenté, samedi à Dakar, son ouvrage consacré à la cybercriminalité, dans lequel il souligne la nécessité d’un cadre juridique approprié permettant de trouver «des solutions originales» à ce phénomène.

Intitulé «Le traitement de la cybercriminalité devant le juge : l’exemple du Sénégal», cet ouvrage édité par les éditions L’Harmattan (France), tente, selon son auteur, d’apporter des éléments de réponse au plan juridique à la lutte contre la cybercriminalité.

«Il s’agit d’apporter des éléments de réponse au plan juridique dans la lutte contre la cybercriminalité», a-t-il expliqué lors de la cérémonie de dédicace, en présence de magistrats, d’avocats et d’un public composé notamment de membres de sa famille.
«Il n’est pas possible d’apporter des réponses techniques ou économiques mais l’ouvrage a tenté d’apporter des réponses juridiques à la cybercriminalité mais une fois devant le juge», a dit l’auteur.
«On pensait que la cybercriminalité est un mythe pas une réalité mais à la réflexion, on se rend compte que c’est un phénomène réel. Ce sont les études rendues par les juridictions qui ont permis de se rendre compte de l’existence du phénomène», a-t-il souligné.
«Nous avons insisté sur la nécessité d’avoir un cadre juridique approprié. Le Sénégal l’a déjà, mais il est important d’avoir un juge qui ose aller au-delà des faits pour trouver des solutions originales au phénomène de la cybercriminalité», a indiqué Pape Assane Touré.

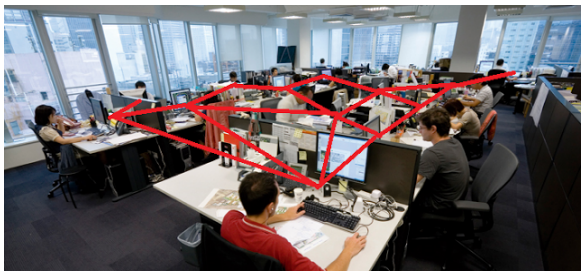
Selon le magistrat, conseiller technique au ministère de la Justice, le législateur seul ne peut apporter des réponses concernant par exemple le piratage dans le domaine informatique.

«Les instances juridiques, les intermédiaires de l’Internet, les conditions d’accès, d’hébergement voire tous les acteurs doivent aller ensemble pour trouver une réponse globale et définitive à la cybercriminalité», a-t-il déclaré.
Intervenant lors de cette cérémonie de dédicace, le garde des Sceaux, ministre de la Justice, Sidiki Kaba, a soutenu que cette publication offre «une bonne base» pour aller de l’avant, comprendre les instruments et les outils pour une répression adéquate de la délinquance.
«La cybercriminalité est une des formes modernes de la délinquance que nous avons pu voir avec l’avènement de la société numérique. Et on ne peut pas utiliser des instruments classiques contre ces personnes qui commettent ces crimes», a-t-il dit, estimant que l’ouvrage ouvre notamment une perspective sur la prévention.
Le ministre de la Justice n’a pas tari d’éloges à l’endroit de l’auteur, le qualifiant de praticien et théoricien du droit tout à la fois. »Et cela est difficile à avoir, parce que c’est deux domaines différents», a-t-il commenté.
Selon Me Sidiki Kaba, le magistrat Pape Assane Touré participe à la pratique du droit, à la construction de la jurisprudence, soulignant que la cybercriminalité est l’avenir du droit.
APS

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.senenews.com/2014/11/23/un-livre-consacre-a-la-cybercriminalite-souligne-la-necessite-dun-cadre-juridique-approprie_96296.html

A quand le premier virus informatique acoustique ? ~ Sweet Random Science

	A quand le premier virus informatique acoustique ?

Je sais qu'ils sont payés pour cela, mais quand même : où diable vont-ils pêcher toutes ces idées ? Après la démonstration du Stanford Security Laboratory sur la façon dont les capteurs peuvent servir à espionner, voire détourner nos téléphones portables, des experts en informatique de l'institut Fraunhofer FKIE ont mis au point un protocole de transmission acoustique : des ordinateurs, pourvus qu'ils soient assez proches les uns des autres, peuvent communiquer via leurs haut-parleurs et microphones, à des fréquences inaudibles pour l'Homme, sans que cette activité ne soit détectée par les moyens de protection classiques.

Une idée qui semble relever de la science-fiction, même si la possibilité de la transmission acoustique avait déjà été proposée pour expliquer la mystérieuse persistance du malware polémique BadBIOS.

Dans leur article, publié le mois dernier dans Journal of Communications, Michael Hanspach et Michael Goetz exposent la méthode qui leur a permis de réaliser cette prouesse : en adaptant un système qui avait été imaginé pour établir des communications sous l'eau, ils sont parvenus à transmettre des informations sur des distances d'une vingtaine de mètres. Les signaux sont modulés en ondes sonores à une fréquence proche de celles des ultrasons, et sont donc inaudibles pour l'oreille humaine. Les chercheurs démontrent que cette méthode peut être utilisée pour établir un véritable réseau par lequel peuvent transiter des informations comme des mots de passe ou des identifiants de connexions, notamment lorsqu'ils sont saisis sur le clavier.

La vitesse de transmission, de l'ordre de 20 bits par seconde, ne permet évidemment pas de transmettre directement un document mais elle pourrait être suffisante pour placer une commande simple : désactiver une protection et envoyer un document par mail par exemple. De quoi rendre complètement inutiles les mesures de précaution d'isolement physique de certains site sensibles, comme les bases miliaires, les centres de services secrets ou les centrales nucléaires.

Dans une des expériences, Hanspach et Goetz établissent un réseau dans les propres locaux du Fraunhofer Institute for Communication, Information Processing and Ergonomics. Un espace de travail ouvert peut donc devenir un réseau d'échange à l'insu des utilisateurs et des logiciels anti-virus. Ce réseau serait accessible via n'importe quel terminal en mesure d'émettre et de capter des sons : un téléphone portable par exemple.

Utilisé de façon malveillante, ce système permettrait d'infiltrer un réseau, récupérer des mots de passe et les transmettre à des tiers, sans provoquer la moindre réaction des dispositifs de protection. Les anti-virus se concentrent en effet sur les modes de communication plus classiques et seraient totalement impuissants face à une attaque de ce genre.

Une faille qui sera sans doute corrigée rapidement, avec l'ajout d'un système anti-intrusion basé sur l'analyse des signaux audio émis et reçus. En attendant, on peut tout simplement désactiver les composants audio ou brider les haut-parleurs en supprimant la transmission des hautes fréquences.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://sweetrandomscience.blogspot.fr/2013/12/a-quand-le-premier-virus-informatique.html

Paiement par mobiles : Trop peu de sécurité face au piratage

Paiement par mobiles : Trop peu de sécurité face au piratage

Dans ses prédictions de sécurité pour les années à venir, Trend Micro fait un point sur la multiplication des nouveaux moyens de paiement et leur impact potentiel en termes de cybercriminalité.

Le paiement mobile et sans contact
Le lancement d'Apple Pay ou de Google Wallet sont la preuve de l'évolution des usages des consommateurs, désormais prêts à payer directement depuis leur mobile. Cependant, les terminaux mobiles sont toujours peu sécurisés.
Les solutions existantes sont encore trop rarement utilisées par les mobinautes qui n'ont pas pleinement conscience des risques, bien que les cybercriminels ne cessent de perfectionner leurs techniques pour tirer profit de ces nouveaux outils. A titre d'illustration, CurrentC, projet d'un consortium de distributeurs américains pour concurrencer Apple Pay, a récemment été piraté et ce, avant même d'avoir été lancé.

La technologie NFC, largement utilisée dans les solutions de paiement mobile, va ainsi continuer d'être l'objet d'une attention toute particulière des pirates. Les utilisateurs de Google Wallet l'ont déjà appris à leurs dépens lorsqu'une application malveillante, à laquelle des privilèges NFC avaient été accordés, s'est montrée capable de dérober les informations de leur compte utilisateur et leur argent.

« Le NFC s'impose de plus en plus or aujourd'hui, si l'on parle de sécurité, ni les utilisateurs, ni les fabricants d'équipements mobiles ne semblent vraiment prêts », commente Loïc Guézo, de chez Trend Micro. « Les utilisateurs doivent prendre conscience que les attaquants vont se donner les moyens d'intercepter les tags NFC en transit, et se montrer prudents. De leur côté, il est essentiel que les fabricants prennent des mesures et envisagent la sécurité des produits dès leur conception. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lafibreoptique.com/focus/20112014,cybercriminalite-des-terminaux-mobiles-peu-securises,1920.html

---

Une ville victime de Cyberattaques. Ottawa ciblée, Toronto menacée

Une ville victime de Cyberattaques. Ottawa ciblée,

«Anonymous» attaque le site de la Ville d'Ottawa
Un pirate informatique qui dit faire partie du groupe Anonymous a menacé dimanche de cibler les sites web appartenant à la Ville et à la police de Toronto.

Cette menace en ligne provient d'un présumé pirate appelé Aerith. Il s'agit du même internaute qui aurait paralysé le site internet de la Ville d'Ottawa, vendredi soir. La page en question affichait alors une image d'une banane dansante et un message menaçant envers un policier d'Ottawa.

Aerith a également revendiqué les problèmes informatiques ayant paralysé ce week-end le site web de la police d'Ottawa. De samedi soir jusqu'à tôt dimanche matin, le site ottawapolice.ca était complètement hors service.
«Notre équipe d'enquête travaille aux côtés de nos experts en technologie de l'information afin d'identifier la source des problèmes techniques qui ont eu lieu la nuit dernière, a indiqué dimanche le chef de la police d'Ottawa, Charles Bordeleau. Notre réseau reste sécurisé», a-t-il assuré.
Le porte-parole de la Ville de Toronto Jackie DeSouza a indiqué que la Ville était au courant de ce qui était arrivé à Ottawa. Les fonctionnaires «demeurent très vigilants» et surveillent toute activité suspecte sur le site toronto.ca, a-t-il assuré.
Le compte Twitter de Aerith – qui indiquait, probablement à tort, avoir été fondé en Turquie – a été suspendu depuis les possibles cyberattaques.
Le groupe Anonymous s'en prendrait ainsi à la Ville d'Ottawa pour défendre la cause d'un adolescent de Barrhaven, en banlieue de la capitale nationale. Ce dernier fait face à 60 chefs d'accusation pour avoir fait de faux appels rapportant des menaces à la bombe, des prises d'otages ou des fusillades, tout en imitant la voix d'une autre personne, généralement un rival de la communauté de jeu en ligne.
Les attaques informatiques revendiquées par «Anonymous» seraient en lien avec une nouvelle preuve qui n'aurait pas été retenue par les enquêteurs et qui démontrerait que l'adolescent de Barrhaven n'est pas responsable des méfaits, mais qu'il s'agit plutôt d'un homme du New Jersey. La police de Toronto aurait déposé quelques-unes des 60 accusations.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://fr.canoe.ca/techno/nouvelles/archives/2014/11/20141123-175629.html

Licencié pour un abus d'utilisation de l'email perso en entreprise ? Voici un levier de contestation !

Licencié pour un abus d'utilisation de l'email perso en entreprise ? Voici un levier de contestation !

L'employeur qui n'a pas déclaré préalablement à la CNIL son système de surveillance des salariés ne peut pas en utiliser les données récoltées pour sanctionner ou licencier un salarié pourtant fautif.

Dans un arrêt en date du 8 octobre 2014, n° 13-14991, la Cour de cassation a jugé que des informations collectées via un système de traitement automatisé de données personnelles ne pouvaient être utilisées par l'employeur à l'appui d'un licenciement dès lors que le dispositif n'avait pas encore été déclaré à la Cnil.
En l'espèce, l'employeur n'avait pas omis de déclarer le système de surveillance à la Cnil, mais l'avait déclaré tardivement, à savoir près de 2 mois et demi après sa mise en place. Ce dispositif avait toutefois servi dès son installation à mettre en lumière l'utilisation excessive par une salariée de sa messagerie professionnelle à des fins personnelles.
Si » le système de surveillance permettait de prendre connaissance non pas du contenu des messages mais de la date et de l'heure d'envoi ou de réception, de leur destinataire ou expéditeur et de leur objet. Il avait ainsi comptabilisé, sur une période de 2 mois, un peu plus de 1200 messages personnels envoyés et reçus par la salariée via sa messagerie professionnelle » rappelle un auteur.

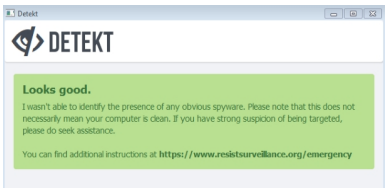
La Cour de cassation invalide le licenciement de la salariée fondé sur une utilisation abusive de la messagerie électronique durant les 2 mois ayant précédé la déclaration du dispositif de surveillance à la Cnil, considérant que « constituent un moyen de preuve illicite les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la Cnil ».
Par Me Grégoire HERVET

Et vous ? Vous en pensez quoi ?
Cliquez et laissez-nous votre avis…

Source : http://www.juritravail.com/Actualite/obtenir-des-dommages-et-interets-pour-licencenciement-pour-faute-grave-ou-lourde-injustifie/Id/170721

Déception : on a testé

Detekt, il ne s’est rien passé



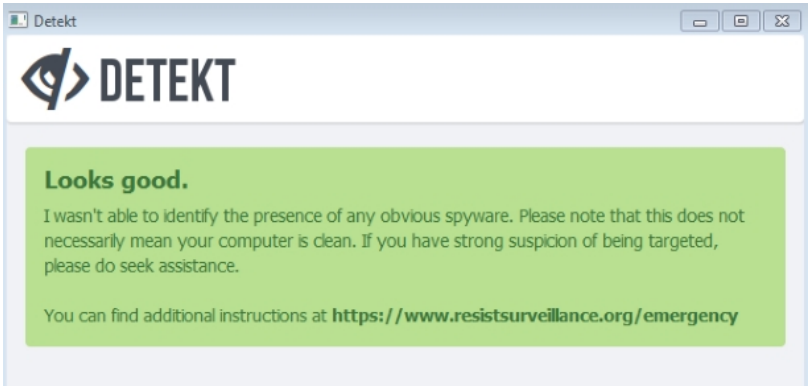
Déception : on a testé Detekt, il ne s’est rien passé

La promesse était belle : Detekt scanne votre ordinateur à la recherche des logiciels espions qui ciblent les activistes de tout poil, les minorités religieuses, et les journalistes. Nous avons essayé. Ça semble marcher, mais on est un peu amer.

Développé pendant deux ans par Claudio Guarnieri (un informaticien basé à Berlin) en partenariat avec Amnesty International et l'EFF entre autres, Detekt est un logiciel gratuit dont la promesse est d'informer l'utilisateur sur les spyware qui se seraient potentiellement glissés dans sa machine.

« Les défenseurs des droits de l'homme, les journalistes, les ONG, les opposants politiques, les minorités religieuses ou ethniques » sont particulièrement ciblés par les agences de renseignement qui utilisent des outils numériques d'espionnage, avertit l'auteur du logiciel.

La rédaction s'est donc prêtée au jeu du test. Après tout, savoir être espionné par la NSA, la DGSE ou Kim Jong-un, ça crédibilise notre travail.



(Personne ne nous espionne)

Après un scan offline de la machine, le verdict tombe. Rien de suspect sur l'ordinateur utilisé pour rédiger cet article. D'où deux propositions qui nous chagrinent : nous n'entrons dans aucune des catégories espionnées sus-nommées, ou bien nous sommes totalement inoffensifs pour les dites agences de renseignement. Préférons dire que nous avons beaucoup de chance.

En cas de détection d'un danger, l'auteur de Detekt mentionne que le nettoyage reste à faire soi-même. Detekt avertit, mais ne soigne pas. Par ailleurs, s'il ne trouve rien, cela ne signifie pas nécessairement que l'ordinateur ne soit pas la cible d'un service espion, mentionne le site de Detekt (ndlr. ouf !).

Programmé en Python, Detekt recherche des chevaux de Troie de certaines familles, comme DarkComet RAT, XtremeRAT, BlackShades RAT, njRAT, FinFisher FinSpy, HackingTeam RCS, ShadowTech RAT et Gh0st RAT. L'acronyme RAT signifie ici Remote Access Trojans. Le fichier readme.md donne d'autres informations techniques.

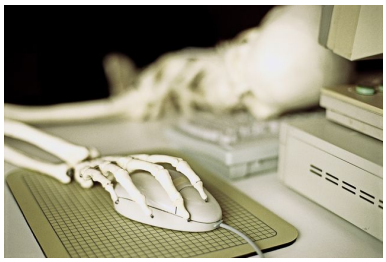
Au delà de cette annonce, qui est assurons-le une initiative salutaire, se pose la question de la pérennité de ce type de solution. Tout comme les antivirus, les anti spyware ne sont efficaces que s'ils sont régulièrement mis à jour, pour intégrer les nouvelles menaces, et celles déjà recensées, mais qui évoluent.

Et vous ? Vous en pensez quoi ?

Cliquez et laissez-nous votre avis…

Source : http://www.zdnet.fr/actualites/deception-on-a-teste-detekt-il-ne-s-est-rien-passe-39809965.htm

Technologie: Le numérique a la mort aux trousses



Technologie: Le numérique a la mort aux trousses

Aurore est décédée. C'était il y a cinq ans. Pourtant, son profil Facebook, lui, vit toujours. Ses proches l'ont transformé en mausolée. Untel poste une photo, un autre se fend d'un mot souvenir. Le tout ne serait pas choquant si le réseau social n'envoyait pas chaque année une alerte anniversaire à ses «amis». L'internaute ne meurt-il donc jamais?

Avec le développement des technologies digitales, la question de la mort numérique s'invite dans le débat, entraînant avec elle une foule de questions: que deviennent nos données numériques (mails, réseaux sociaux, photos…) lorsque l'on passe de vie à trépas? Peut-on hériter d'une bibliothèque iTunes comme on récupérait les vinyles de grand-père? Les morts du Web ont-ils le droit de reposer en paix? «Le sujet reste encore très peu encadré par la loi, souligne le conseiller national Jean Christophe Schwaab, c'est pourquoi j'ai décidé de déposer un objet parlementaire en septembre dernier, afin que le droit de succession s'intéresse enfin aux données numériques.» L'enjeu est de taille. Selon la Commission nationale de l'informatique et des libertés (Cnil), un profil Facebook sur cent – soit 130 millions de pages – appartiendrait à un mort.

Et vous ? Vous en pensez quoi ?
Cliquez et laissez-nous votre avis…

Obligation de résultat pour une agence de référencement de Sites Internet. Jurisprudence en vue ?

Obligation de résultat pour une agence de référencement de Sites Internet. Jurisprudence en vue ?

Par un jugement du 28 octobre 2014, le Tribunal de commerce de Paris a condamné un prestataire à rembourser son client pour n'avoir pas amélioré le référencement de son site.

Le tribunal a appliqué une clause du contrat de référencement par lequel le prestataire s'était engagé à atteindre « un positionnement minimum sur 50 % » des expressions clés convenues dans les deux premières pages des moteurs de recherche d'ici la fin de l'année de la prestation.

Or, le positionnement du site sur les moteurs de recherche avait diminué.
Le client avait donc demandé le remboursement du contrat, pour non respect de ses engagements.
Au contraire, le prestataire estimait que l'obligation de résultat prévue initialement au contrat s'était transformée en obligation de moyen, du fait d'un manque de collaboration du client.

Outre le fait que le contrat prévoyait bien un obligation de résultat, le Tribunal de commerce n'a pas suivit cette argumentation car il a estimé que le prestataire n'avait pas apporté la preuve que le client n'avait pas été suffisamment rapide et réactif. De plus, le Prestataire ne s'était jamais plaint du manque de rapidité et de collaboration du client lors de l'éxécution du contrat de référencement. Le Prestataire n'avait, par ailleurs, pas réagi au problème de lien retour que subissait le site, alors qu'il était connu depuis de nombreux mois.
Ce jugement rappelle de porter une attention toute particulière aux obligations du prestataire dans les contrats de référencement.
A partir du moment ou un clause est chiffrée, elle peut devenir une obligation de résultat et non une simple obligation de moyens…
Définitions :
Obligation de moyens :
L'obligation de moyens (Article 1137 du Code civil) est une obligation en vertu de laquelle le débiteur doit déployer ses meilleurs efforts pour atteindre l'objectif visé ; elle s'oppose à l'obligation de résultat, par laquelle un objectif est donné. Il s'agit d'une d'une appréciation site 'in abstracto', c'est-à-dire en référence à un modèle abstrait de « l'Homme raisonnable ».
La responsabilité du débiteur d'une obligation de moyens ne peut être engagée du seul fait qu'il n'a pas atteint un résultat (chiffré par exemple). Dans cette éventualité, c'est au créancier de démontrer que le débiteur n'a pas été assez diligent dans sa tentative d'exécution de son obligation.
Par contraste, la responsabilité du débiteur au titre d'une obligation de résultat pourra être engagée sur la simple constatation que le résultat convenu n'a pas été atteint. Le débiteur ne peut s'exonérer de sa responsabilité qu'en prouvant la survenance d'un cas de force majeure.

Obligation de résultat :
Obligation pour le débiteur d'atteindre un résultat précis.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.avocat-rainio.com/amelioration-du-positionnement-obligation-de-resultat-a-respecter.html