Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

# S.A.S.

# WEB 2.0

# AJAX

# FILES

# WIRELESS

INTERNATIONAL
PAGE 10

SPÉCIAL SÉCURITÉ AU QUEBEC

N°003 - Prix : 18 € - Trimestriel : avril, mai, juin 2008

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

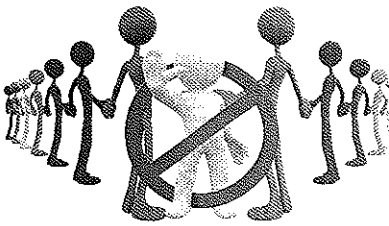
# SOMMAIRE

THÉMA

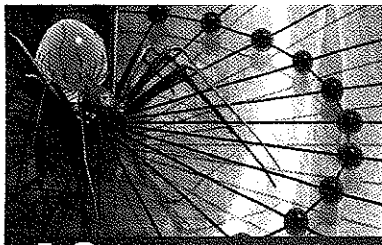
**26 SAS**



**10 QUÉBEC : UN MARCHÉ EN DEVENIR**



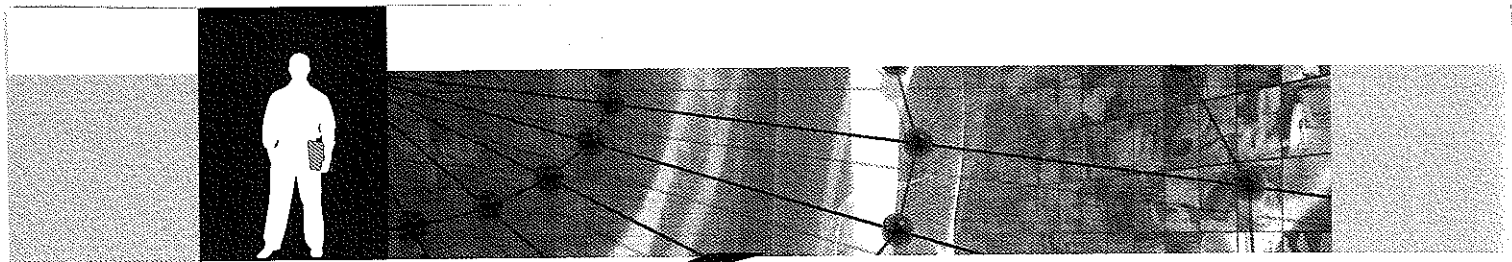
**44 MALWARE BUSTERS**



**48 WEB 2.0**

**54 BUSINESS INTELLIGENCE**

**80 SÉCURITÉ PHYSIQUE**

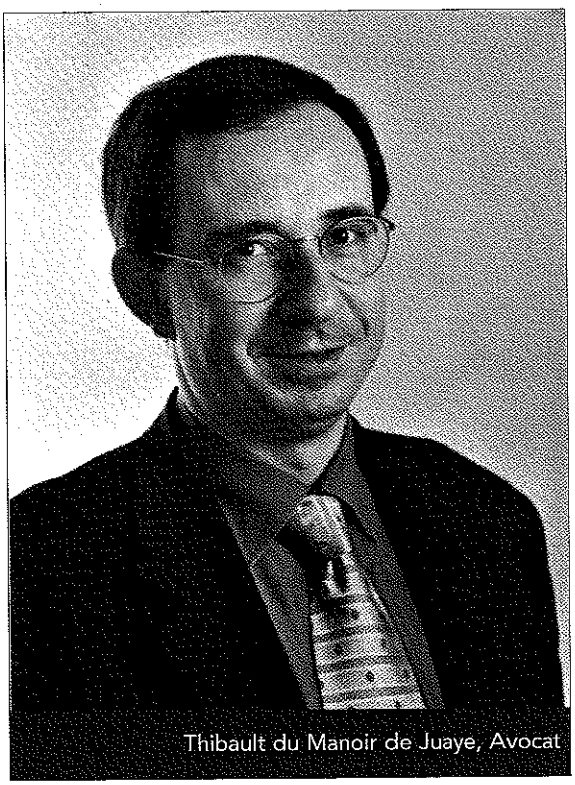


THÉMA

# A QUI PEUT-ON CONFIER LES CLEFS DU COFFRE-FORT ?

*Plusieurs sociétés informatiques proposent la prise en charge de la sécurité. C'est la SAS « Security As a Service ». Les arguments qu'elles avancent peuvent paraître séduisants : la sécurité est de plus en plus l'affaire d'hyperspécialistes que les entreprises peuvent ne pas posséder en interne et il peut y avoir une mutualisation des coûts. Cette nouvelle pratique constituée par la SAS suscite des questions juridiques multiples parfois communes à d'autres situations informatiques et sur lesquelles il n'y a pas de décisions de jurisprudence notoires. Il convient donc de se demander ce que pourrait contenir un contrat déléguant la sécurité à un tiers et ce qu'il advient des salariés de l'entreprise cliente à qui était confiée antérieurement la sécurité.*

PAR THIBAULT DU MANOIR DE JUAYE, AVOCAT À LA COUR



Thibault du Manoir de Juaye, Avocat

## Contrat de SAS : attention aux usages non professionnels des salariés

Confier à un tiers sa sécurité nécessite de s'être préalablement entouré du maximum de garanties possible. La description des prestations à envisager ne semble pas poser de difficultés particulières : mise en place de firewall, d'antivirus, « scanning régulier ». Cependant, il faut également viser dans ce type de contrat les usages non purement professionnels que pourraient faire les salariés de leurs postes de travail. D'autres points du contrat doivent être examinés avec plus d'attention.

## Le prestataire informatique est-il tenu d'une obligation de moyen ou de résultat ?

Pour bien appréhender ces concepts juridiques, il convient de les définir. Ainsi, lorsque le prestataire n'est tenu que d'une obligation de moyen, l'entreprise cliente doit alors prouver que le prestataire n'a pas fait tout ce qui était en son pouvoir pour lui donner satisfaction.
Lorsque, en revanche, le prestataire est tenu d'une obligation de résultat, le chef d'entreprise client du prestataire n'aura qu'à établir que le résultat escompté n'a pas été obtenu.
Aucune décision de justice n'a été prise sur la « SAS »

et il est tentant de se reporter aux arrêts et jugements pris dans le cadre d'autres prestations informatiques.
La cour d'appel de Reims a également en avant la notion de « profane en informatique » pour mettre une obligation de résultat à la charge du prestataire en ce qui concerne, par exemple, l'opération technique de transfert de données qui s'était mal déroulée (CA Reims, ch. civ., sect. 1, 2 mai 2006, SARL MS Informatique c/ SARL Quincaillerie Martin : Juris-Data n° 2006-304875).
A contrario, l'obligation de maintenance qui incombe à celui qui, dans le cadre d'un contrat de prestations de services, s'est engagé à maintenir en état de bon fonctionnement des logiciels et à mettre en œuvre tous les moyens pour remédier aux anomalies est considérée comme une obligation de moyen (CA Rouen, 1re ch., 27 avr. 2005 : Juris-Data n° 2005-272233).
Difficile de s'y retrouver.
Une solution mixte sera peut être trouvée par la jurisprudence pour les contrats dans lesquels le prestataire informatique serait tenu d'une obligation de résultat sur les failles de sécurité connues et de moyen sur celles qui sont nouvelles. La difficulté va résider sur le caractère de nouveauté. Ce caractère pourra être défini par contrat, où il sera précisé que toute faille devra être supprimée dans un délai de « xx » heures après qu'elle eut fait l'objet d'un communiqué ou qu'elle eut été découverte.

## Le prestataire peut-il s'exonérer de toute responsabilité ?

Un prestataire pourra être tenté de s'exonérer totalement de sa responsabilité en précisant qu'il ne peut être tenu de réparer les différents dommages survenus du fait de sa défaillance.
Toutefois, de nombreuses décisions ont rappelé qu'une clause d'exonération ne devait pas vider le contrat de son contenu, c'est-à-dire qu'un prestataire se doit de réaliser ses engagements et qu'il est responsable des défaillances.
Ainsi, par exemple, un prestataire informatique a engagé sa responsabilité malgré une clause limitative de responsabilité, dès lors que celui-ci avait installé des versions d'un logiciel antérieures et n'a jamais procédé à la version promise. La cour d'appel de Versailles (1) avait dans un premier temps retenu la responsabilité de l'éditeur de logiciel mais elle avait limité le montant de l'indemnisation à la hauteur du montant prévu par la clause limitative de responsabilité. La chambre commerciale de la Cour de cassation avait alors cassé l'arrêt d'appel considérant que le comportement caractérisait « un manquement à une obligation essentielle de nature à faire échec à l'application de la clause limitative de réparation » (2).

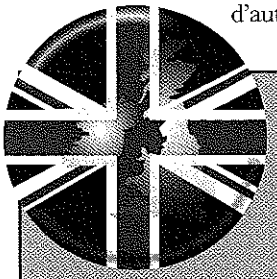
## Les incidents doivent être signalés le plus rapidement possible

Une agression sur le système informatique d'une entreprise peut-être le fait du hasard, par exemple un virus qui serait téléchargé à l'insu d'un des salariés.
Elle peut également résulter d'une volonté délibérée d'un tiers, d'un concurrent qui souhaiterait, par exemple, entrer dans le système.
C'est ainsi qu'un salarié avait été licencié à la suite de l'installation par celui-ci d'un logiciel destiné à permettre la gestion d'un canal de communication sur l'ordinateur depuis l'extérieur de l'entreprise. Or, une telle installation devait nécessairement être subordonnée à une autorisation de l'administrateur système et ne pouvait être laissée à la seule initiative du salarié qui n'avait pas la qualité pour le faire; en mettant en place un accès direct à son ordinateur depuis l'extérieur, il contournait les règles de sécurité en vigueur dans l'entreprise (3). Ces multiples intrusions doivent êtres signalées sans retard pour que les responsables de l'entreprise cliente puissent vérifier si elles ne sont pas orchestrées avec d'autres agressions.

(1) CA Versailles, 12e ch., 31 mars 2005, cité in Un an de droit des contrats informatiques : Comm. com. électr. 2006, chron. 4, par H. Bitan)

(2) Cass. com., 13 févr. 2007, n° 05-17.407, sté Faurecia sièges d'automobiles, SA c/ sté Oracle France, société par actions simplifiée et a : Juris-Data n° 2007-037369.

(3) Cour d'appel PARIS 12 Octobre 2004 SA TELEPERFORMANCE France GIBOUDEAUX Numéro JurisData : 2004-257111)



### WHO CAN BE TRUSTED WITH THE KEYS TO THE VAULT?

*BY THIBAULT DU MANOIR DE JUAYE, ATTORNEY-AT-LAW*

Several IT companies offer security outsourcing services or Security as a Service (SAS) as it is known. The sales arguments are attractive i.e. security is more and more a highly specialised business and it is not possible for companies to possess all the necessary in-house expertise. Outsourcing also allows fixed costs to be spread over a greater number of users. The advent of SAS raises a number of legal questions, some of which are common to other IT situations and for which there is no generally accepted jurisprudence. The question of what to put in a third-party security contract is therefore open as is the question of what happens to the employees who previously looked after security in the client company.

## Les clauses de confidentialité doivent être clairement édictées dans le contrat...

Le prestataire de sécurité va avoir accès à des informations sensibles. Une clause, classique en matière de contrats informatiques, peut ainsi prévoir l'obligation pour les parties de garder strictement confidentielles toutes informations, quelle qu'en soit la nature, qui ont été portées à leur connaissance dans le cadre du contrat de réalisation du développement spécifique.
Il convient également de compléter cette clause en mentionnant l'obligation pour les parties de veiller au respect de la confidentialité par leurs salariés, collaborateurs, filiales et sous-traitants éventuels.
Indépendamment des clauses de confidentialité qui tombent sous le sens, il convient de se demander si un tel prestataire peut travailler pour deux entreprises concurrentes et s'il convient de lui interdire.

## Inclure les données personnelles...

Il est inutile de rappeler que tout système informatique d'une entreprise contient de nombreuses données personnelles et qu'il convient de respecter la loi Informatique et Libertés comme les autres dispositions, dont celles du code du travail.
A cet égard, il convient de rappeler, en application des dispositions de l'article 25 de la loi du 6 janvier 1978, que la collecte de données par tout moyen frauduleux, déloyal ou illicite est interdite.

## Et la surveillance des salariés.

Si la mise en place de la sécurité externalisée conduit à une surveillance des salariés, ces derniers devront avoir été avertis. Les moyens mis en œuvre devront être proportionnels au but poursuivi et le comité d'entreprise devra donner son avis, comme c'est le cas pour tout projet technologique.
Compte tenu de la responsabilité croissante du chef d'entreprise et de l'augmentation des litiges pénaux et civils au sein de l'entreprise, il apparaît nécessaire que l'on puisse remonter à l'auteur d'une infraction pour établir clairement les responsabilités.
Cette traçabilité, dont la mise en œuvre doit se faire dans le respect des droits des salariés, devra également être imposée au prestataire à qui cette tâche a été confiée.

## Le prestataire peut-il s'exonérer de sa responsabilité en invoquant la faute de l'entreprise cliente ?

Par exemple, un prestataire pourra être tenté, comme cela s'est vu, d'exonérer sa propre responsabilité en invoquant la faute de l'entreprise et l'absence de disposition contractuelle écrite suffisamment explicite justifiant une mise en jeu de sa responsabilité du fait de la faute alléguée.
Dès lors, le contrat devra soigneusement préciser ce que le prestataire attend de son client en termes de formation et d'usage de l'informatique pour les salariés, ces derniers étant également sources de vulnérabilité.



## Transfert des salariés dont l'activité est externalisée ?

Si l'on confie à un prestataire externe une mission, que vont devenir les salariés à qui cette tâche était dévolue antérieurement ?
L'article L. 122-12, alinéa 2, du Code du travail prévoit que s'il survient une modification dans la situation juridique de l'employeur, notamment par succession, vente, fusion, transformation du fonds, mise en société, tous les contrats de travail en cours au jour de la modification subsistent entre le nouvel employeur et le personnel de l'entreprise.
En réalité, tout va dépendre de la notion d'entité économique transférée. Peut-on considérer que les services de sécurité informatique sont indépendants du reste de l'entreprise ? Cela paraît difficile. Rappelons à toutes fins utiles les complications rencontrées par la société Alcatel.
Le Conseil des Prud'hommes de Paris dans un jugement du 23 février 2005 a décidé d'annuler une opération d'externalisation conduite par Alcatel Réseaux Entreprise (ARE) avec pour conséquence la réintégration de 328 de ses anciens salariés et ce cinq ans après l'opération.
En l'espèce, cinq ans après l'opération d'externalisation, l'infogérant était en liquidation judiciaire et avait licencié les salariés. Ces derniers ont saisi la juridiction prud'homale et ont obtenu leur réintégration au sein d'ARE.
Le tribunal a, en effet, considéré que l'opération n'était qu'une simple externalisation de personnel, lequel continuait à être contrôlé par le client à travers un contrat de sous-traitance (contrôle des formations et des compétences, clause de non concurrence, attribution de primes...).