

Paris, le 23 novembre 2006

Dans le cadre de la première Université d'Automne des Correspondants Informatique & Libertés, nouvelle manifestation créée par l'AFCDP, le groupe de travail « Cybersurveillance » a présenté lors d'un atelier intitulé « Correspondant et Administrateurs techniques ; Ennemis ou Amis ? » les fruits de ses réflexions.

Rédacteurs principaux:

Odile CAMPERVEUX, Responsable Juridique des Services Informatiques de la Chambre de Commerce de Paris - CIL (ocampserveux@ccip.fr) et

Bruno RASLE, co-animateur du groupe de travail Cybersurveillance (bruno_rasle@halte-au-spam.com)

CORRESPONDANT INFORMATIQUE & LIBERTES ET ADMINISTRATEURS TECHNIQUES : quelle coopération ? *Administrateurs techniques ; Droits & Devoirs*

Un Correspondant Informatique & Libertés dont le champ d'action a été étendu à la Cybersurveillance peut-il mener à bien ses missions sans établir une forme quelconque de relations avec les Administrateurs techniques ? Si contact il y a, quelles en seraient la finalité et la forme ? Quel aide peut en attendre le Correspondant ? Cette note de synthèse est extraite du projet de livre blanc « Le Correspondant Informatique & Libertés et la Cybersurveillance », sur lequel œuvre le groupe de travail éponyme de l'AFCDP.

Un Administrateur ou des Administrateurs ?

En informatique, on désigne par le terme *Administrateur* un professionnel qui a pour métier de gérer techniquement, d'exploiter, de configurer, de maintenir, de sécuriser une ressource informatique.

Il en existe de différents types, selon la ressource qu'ils ont à gérer :

- Administrateur réseau,
- Administrateur système
- Administrateur de messagerie,
- Administrateur de bases de données,
- Administrateur de site web, etc.

Dans les trois premiers cas (Administrateur réseau, Administrateur système et Administrateur de messagerie) la fonction est généralement rattachée à la Direction de l'informatique ou à la Direction des systèmes d'information. En pratique, ils sont sous la responsabilité opérationnelle et hiérarchique d'un RSI (Responsable des Systèmes d'Information), d'un Responsable d'Exploitation, d'un Responsable Réseau, d'un Responsable Système, plus rarement d'un RSSI (Responsable de la Sécurité du Système d'information).

Dans les deux autres cas (Administrateur de bases de données, Administrateur de site web), ils peuvent être, plus rarement, rattachés à un responsable « métiers ».

Exemples ;

- un administrateur de site web rattaché à un service ou direction de la communication
- un administrateur de base de données rattaché à la DRH

Les services généraux peuvent également disposer d'Administrateurs techniques, en charge de la gestion des PABX (et iPBX dans le cas de téléphonie sur IP) et des systèmes de contrôle d'accès aux locaux.

Ces personnels sont de formation technique uniquement. Relativement rares sont les cursus qui intègrent des modules juridiques comportant une réelle sensibilisation à la loi Informatique & Libertés, et plus particulièrement aux « droits et devoirs » des futurs Administrateurs Techniques¹.

Il convient d'être conscient que, relativement fréquemment, surtout au sein des grandes entreprises, les Administrateurs peuvent être externes à l'organisme (prestataires).

La mission de l'Administrateur technique

La mission des Administrateurs consiste à assurer le fonctionnement optimal des ressources informatiques dont ils ont la charge. Ces ressources doivent pouvoir rendre le service pour lesquels elles sont été conçues, avec la qualité, la disponibilité et la performance requises.

Pour atteindre cet objectif, **l'Administrateur doit assurer la sécurité du dispositif** géré et notamment empêcher

- toute intrusion susceptible de modifier, de détruire ou de révéler l'information à des tiers qui ne doivent pas en avoir connaissance,
- l'introduction de programmes malveillants au sein de l'organisme (*malware*),
- les usages abusifs des outils informatiques qui peuvent impacter leur bon fonctionnement².

L'Administrateur s'appuie de plus en plus sur une politique de sécurité, élaborée avec le concours du RSSI ou une direction de l'organisation, qui définit :

- les règles et les procédures à mettre en œuvre dans les différents services,
- les actions à entreprendre et les personnes à contacter en cas de détection d'une infraction (intrusion, exposition de données, infection, etc.)

NB : Il peut être amené à proposer des indicateurs d'alerte, contribuer à la politique d'accès et à la définition de la politique de sécurité

¹ Signalons toutefois – entre autres – les initiatives de l'EPITA, de l'ENSTA (Ecole Nationale Supérieure de Techniques Avancées) et de l'ESIEE (Ecole Supérieure d'Ingénieurs en Électronique et Électrotechnique).

² Outre pour ces motivations, la sécurité informatique est également recherchée pour respecter le cadre légal (Informatique & Libertés, Loi Godfrain, LSF, Sarbanes-Oxley, etc.), pour conserver le positionnement concurrentiel de l'entité, ou pour éviter des pénalités (Data Security Payment Card Industry) dans un cadre contractuel.

Pour assurer la sécurisation du dispositif dont ils ont la charge, **les Administrateurs ont techniquement accès** :

- à l'ensemble des données (fichier de logs, contenu des bases de données),
- à l'ensemble des informations relatives aux utilisateurs (profil, droit d'accès et droit d'usage)³,
- aux messageries, et même à leur contenu

S'il est partie prenante d'un dispositif de cybersurveillance, et afin d'opérer un contrôle efficace – mais respectueux des droits et des personnes – l'Administrateur doit suivre plusieurs principes :

- Sa démarche doit être impartiale et sincère. Il doit agir dans le cadre de ses fonctions et son action ne doit pas découler d'une initiative personnelle ou d'un ordre hiérarchique mais d'une nécessité justifiée par des impératifs de sécurité. Il lui appartient également d'agir dans le respect de la vie privée des salariés.
- Sa démarche doit se faire aussi dans une logique de transparence vis à vis des salariés. Ces derniers doivent être informés par l'employeur de la mise en place d'un dispositif de contrôle soit en le spécifiant dans le contrat de travail soit au moyen d'une charte informatique.
- Les contrôles, qu'ils soient effectués par le supérieur hiérarchique en vertu de son pouvoir hiérarchique ou par l'Administrateur dans le cadre de sa fonction doivent être proportionnels au but recherché. Il appartient à l'administrateur d'utiliser les moyens permettant de remplir sa mission sans aller au-delà. A titre d'exemple, il n'y a pas lieu pour l'administrateur réseau de contrôler le contenu même des messages émis ou reçus si le seul contrôle du volume des pièces jointes ou des extensions des fichiers joints lui permet de vérifier l'utilisation optimale du réseau. Ou encore, l'inscription à des forums de discussion ou le téléchargement des fichiers non autorisés ne requièrent pas l'ouverture des mails pour prouver le manquement du salarié.

Il revient à l'Administrateur de faire remonter à sa direction des informations relatives à la sécurité (incidents venant de l'extérieur ou de l'intérieur) sous forme de statistiques régulières ou de signalisation ponctuelle.

Dans le respect de l'ensemble des obligations légales (transparence, proportionnalité, etc.), l'Administrateur alerte son employeur sur base de contrôle statistique (sur ce qui constitue « l'enveloppe » des messages électroniques : émetteur, destinataire, objet, taille, nature du fichier attaché, fréquence, etc.) ou sur un filtrage automatisé par mots clés. Il peut avoir accès aux informations des utilisateurs, à savoir leur messagerie, leurs connexions à Internet, les fichiers de journalisations.

NB : Il est souhaitable que l'alerte soit exprimée en respectant un processus interne, formalisé et documenté.

Il dispose de plusieurs moyens de contrôle pour vérifier l'utilisation loyale du réseau ou des outils informatiques.

³ En soit, un tel accès n'est contraire à aucune disposition de la loi Informatique et Libertés, du moment qu'ils opèrent un contrôle loyal, transparent et proportionné.

Il peut, par exemple,

- contrôler les débits,
- identifier la durée des connexions,
- répertorier les sites Web les plus fréquemment visités ou les tentatives de connexion,
- contrôler les extensions des pièces jointes à un message électronique,
- relever leurs volumes,
- suivre le comportement d'un utilisateur (impression, consultation de base de données, transfert de données sur clé USB), etc.

Ces éléments peuvent être autant indices permettant à l'employeur de

- renforcer ou ajuster la politique de sécurité,
- compléter la sensibilisation des utilisateurs
- au pire, de saisir la justice afin qu'elle accède aux traces informatiques et au contenu des messages ou fichiers du salarié. Le recours à justice de l'employeur se fonde alors sur l'avertissement donné par l'Administrateur et la révélation d'indices graves, sans toutefois que ce dernier ne puisse révéler le contenu des messages ou fichiers.

Par contre, si la préoccupation de la sécurité du système d'information justifie que les Administrateurs fassent usage de leur position et des possibilités techniques à leur disposition pour mener des investigations et prendre des mesures que la sécurité impose, en revanche **la divulgation du contenu des messages ne relève pas de cet objectif et constitue une faute** pouvant engager leur responsabilité personnelle ou professionnelle. Les Administrateurs n'ont pas à exploiter, volontairement ou sur ordre de leur hiérarchie, le contenu des fichiers ou de la messagerie des utilisateurs qui se trouvent dans l'espace PRIVÉ du collaborateur, l'ensemble étant couvert par « un droit au respect de l'intimité de la vie privée ; que celle-ci implique en particulier le secret des correspondances » (cf. arrêt Nikon). En outre cette éventuelle communication rend illicite, et donc totalement inefficace, la preuve ainsi obtenue.

Pour mener à bien sa mission sans risquer de transgresser les règles applicables à sa fonction, l'administrateur n'a pas besoin d'avoir accès au contenu des messages et des fichiers des utilisateurs, des bases de données. A cet égard, lors de présentations publiques, les experts techniques de la CNIL recommandent une plus grande ségrégation des accès et des rôles ; pour eux, il n'est pas « naturel » qu'un Administrateur ait accès à tout. Le Correspondant Informatique & Libertés peut donc étudier cette question, en partenariat avec les Administrateurs techniques.

NB : Sur ce sujet, on prendra connaissance avec profit des travaux de la CNIL (La cybersurveillance sur les lieux de travail - rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL, mars 2004) ainsi que ceux du Forum des droits de l'Internet (Rapport Relations du travail et Internet, 2002).

Par ailleurs, il existe des solutions de chiffrement qui permettent de masquer à la connaissance des Administrateurs certains champs sensibles (dont les données à caractère personnel). Ces solutions permettent notamment aux Administrateurs de bases de données (souvent désignés par le terme anglo-saxon, DBA, pour *Data Base Administrator*) de mener à bien leurs missions, sans pouvoir être suspectés d'avoir pris connaissance (et divulgué) des informations sensibles.

Concernant plus spécifiquement les Administrateurs rattachées aux équipes de développement, des outils d'anonymisation des données permettent de créer des jeux de tests

aptes à sortir de la communauté européenne, ou à être utilisés lors de sessions de formation interne.

Enfin, pour éviter les éventuels litiges dans le cadre de processus de cybersurveillance, on notera qu'il existe également des solutions de conservation de données sensibles qui nécessitent une autorisation simultanée multiple pour laisser l'accès aux informations : par exemple, les traces d'utilisation d'Internet d'un collaborateur précis ne pourront être accessibles qu'avec l'accord du responsable fonctionnel, du Correspondant Informatique & Libertés et du représentant du personnel, par exemple. Le recours à ce type de solution participe également de la sécurisation de la position des Administrateurs.

Faut-il signaler les administrateurs parmi les destinataires du traitement ? Nos auditions laissent apparaître que cette précaution n'est généralement retenue que pour des traitements de données sensibles. Pourtant, certains conseils juridiques préconisent de les mentionner systématiquement (sauf, naturellement, si des moyens techniques les empêchant d'avoir accès aux données ont été déployés).

En tout état de cause, il ne s'agit pas de lister les administrateurs nominativement, mais de signaler que cette fonction fait partie des destinataires du traitement. Il appartient au déclarant de donner librement toutes les précisions complémentaires qu'il juge utiles ; nombre, qualité (internes, externes), contrôle d'accès, traçabilité de ces accès, etc.

Le Correspondant pourra, avec profit, consigner cette information dans le registre des traitements dont il a la charge.

La position inconfortable de l'Administrateur

L'administrateur est un salarié qui comme tel est soumis aux consignes de sa hiérarchie. Cependant il doit assurer sa fonction dans le respect des règles juridiques existantes complétées par la jurisprudence sous peine de voir sa responsabilité personnelle engagée. L'exercice de la fonction d'administrateur est à la croisée de ces deux obligations.

Ainsi, une pression particulièrement forte peut être exercée sur l'administrateur par le responsable des traitements en matière de traitement de données à caractère personnel dans la mesure où la loi Informatique & Libertés l'oblige à protéger de façon adéquate ce type de données.

Coincés entre leur direction, qui peut en arriver à exiger l'accès au contenu des e-mails des collaborateurs ou à demander à transgresser les obligations légales en matière de cybersurveillance et leur souci de participer à la protection du système d'information de son entreprise, ces administrateurs disposent d'une marge de manœuvre étroite, ce qui rend leur position inconfortable.

Préconisation AFCDP :

À titre de précaution, il est recommandé que les Administrateurs en place disposent d'une définition écrite de leurs missions sous la forme d'une annexe au contrat de travail, d'une lettre de mission ou au mieux d'une charte spécifique faisant apparaître en particulier la clause de confidentialité et sa nécessaire discrétion (non divulgation au sein de l'entreprise, y compris à sa hiérarchie et à ses collègues, des informations personnelles qui concernent un salarié dont il peut avoir connaissance dans le cadre de ses fonctions).

Préconisation AFCDP :

Il est recommandé d'indiquer dans la charte « d'usage des moyens informatiques » à destination des salariés, les caractéristiques de la fonction d'administrateur afin d'officialiser ses interventions et leur donner une base légale.

A cet égard, la cour d'appel de Paris a reconnu la culpabilité d'un responsable réseau et de son responsable hiérarchique pour avoir diffusé le contenu d'un message intercepté à la suite d'une opération justifiée par des problèmes de sécurité. La Cour a considéré que « *si la préoccupation de la sécurité du réseau justifiait que les administrateurs fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait, par contre la divulgation du contenu des messages ne relevait pas de cet objectif* ».

La cour d'appel a toutefois assorti les peines d'amende d'un sursis considérant que les prévenus étaient « *confrontés à une situation inédite qui perturbait gravement le fonctionnement d'un laboratoire scientifique de haut niveau* » et qu'ils ont agi « *dans l'ignorance probable [...] de leur véritable marge de manœuvre* ». Un pourvoi en Cassation est en cours.

Si dans cette affaire l'Administrateur avait agi sous l'injonction de son responsable hiérarchique, **il semble qu'il existe de nombreux incidents qui impliquent des Administrateurs techniques** : profitant de ses connaissances techniques et de ses prérogatives, l'Administrateur crée un incident imputable à un tiers.

Dans leur très grande majorité, ces incidents sont liés à des mésententes de tous ordres entre collègues de bureau. Ces mésententes n'ont généralement aucun rapport avec les missions des personnes impliquées. Ces « incidents » se résolvent aujourd'hui en interne et ne sont donc pas révélés.

Pour les cas les plus bénins, l'Administrateur se voit simplement rappelé à l'ordre par sa direction. Pour les cas jugés plus choquants par l'entreprise concernée, celle-ci fait part à l'Administrateur qu'elle projette de le licencier, en étant très précis sur le motif. Ces administrateurs préfèrent démissionner et changer d'entreprise plutôt que de risquer de voir cet incident entacher leur carrière⁴.

⁴ À ce jour, aucun cas n'a été relevé au niveau des affaires jugées devant les Prud'hommes.

D'après nos auditions, il semble que les cabinets d'avocats spécialisés soient aujourd'hui fréquemment sollicités

- par des Administrateurs inquiets, qui veulent savoir si ce que leur demande leur direction est bien légal,
- par des entrepreneurs (principalement des PME), qui pensent avoir relevé des pratiques non-respectueuses de la part de leurs Administrateurs techniques, mais ne savent pas quoi faire et comment s'y prendre : ils sont en état de dépendance (risque d'interruption de service, en cas de départ de l'Administrateur, véritable « conscience technique » de l'entreprise)

On rappellera que ces demandes de conseils sont onéreuses.

Pour réduire cette dépendance, certains avocats recommandent aux entreprises d'inclure dans avenant au contrat de travail de l'Administrateur, en sus de la confidentialité, une clause spécifique dite de « réversibilité ». Elle invite l'Administrateur à documenter ses actions (ce qui correspond à une gestion de la connaissance). Dans la pratique, cette réversibilité se traduit par un « état informatique de l'administrateur » que l'entreprise peut faire auditer par un tiers, afin de vérifier a) s'il est à jour, b) s'il est pertinent et c) s'il est conforme à l'état de l'art.

Le Correspondant et les Administrateurs

Lors de la définition de sa mission, le Correspondant prendra soin de s'assurer que les Administrateurs seront bien avertis de sa nomination par le responsable de traitement, et qu'ils seront amenés à collaborer avec lui.

Préconisation AFCDP :

Dès sa prise de fonction, il appartient au Correspondant Informatique & Libertés de prendre contact avec les Administrateurs, afin

- * de valider leurs connaissances relatives à leurs obligations légales,
- * de vérifier que leurs missions n'enfreignent en rien ce cadre,
- * que leurs moyens et processus font de même,
- * de leur dispenser un complément de formation concernant leurs devoirs et leurs droits au regard de la loi Informatique & Libertés,
- * de leur rappeler les règles de sécurisation des données à caractère personnel dont ils ont la charge.

À cette occasion, les Administrateurs bénéficiant en règle générale d'une grande autonomie dans le domaine de la cybersurveillance, le Correspondant portera une attention toute particulière sur ce sujet. Le CIL pourra analyser notamment les processus par lesquels les Administrateurs sont amenés à signaler à leur direction les indices d'éventuels usages abusifs des outils informatiques par le personnel, et en étudier avec eux les possibles améliorations.

Le Correspondant peut participer à l'organisation de la protection des Administrateurs techniques en participant à la rédaction des règles de déontologie de la fonction ou des règles juridiques applicables à la fonction (charte, lettre)

Le Correspondant veille à faire en sorte que les Administrateurs participent activement au respect de la loi Informatique & Libertés au sein de l'organisme ou entreprise. En retour, le Correspondant peut les aider à mieux évaluer leurs risques et à prendre toute mesure destinée à les sécuriser.

Les Administrateurs doivent pouvoir trouver auprès du Correspondant Informatique & Libertés aide et conseil, sur tous les sujets de la compétence de ce dernier, et dans le respect du périmètre de sa mission (le Correspondant veillera donc à ce que ce point soit spécifié dans ses fonctions). S'ils n'ont pas les connaissances requises pour ce faire, ils peuvent consulter le Correspondant Informatique & Libertés.

A titre d'exemple, le CIL pourra éclairer l'Administrateur sur les questions spécifiques concernant l'opposabilité de l'engagement de confidentialité en ce qui concerne la force publique, la Justice, la CNIL, etc. On peut également évoquer la nécessité de vérifier qu'un disque dur contenant des informations à caractère personnel ne sorte de l'organisme à l'occasion d'une intervention menée par un tiers mainteneur.

Les Administrateurs doivent également pouvoir se tourner vers le Correspondant à chaque fois qu'ils se posent la question « *comment réagir face à une situation grave et préjudiciable pour l'entreprise, sans enfreindre la loi ?* »

En conclusion

On conçoit donc qu'une coopération mutuellement profitable doit rapidement s'instaurer entre les Correspondants Informatique & Libertés et les Administrateurs techniques.

Ces derniers y gagneront en sécurisation de leur situation personnelle et en tranquillité d'esprit.

Les premiers bénéficieront de relais indispensable dans leur mission principale : le respect de la loi Informatique & Libertés et la protection des données à caractère personnel.