https://laurentbloch.org/BlogLB/Une-charte-de-l-administrateur-de

Une charte de l'administrateur de système et de réseau

- Zinformatiques - Sécurité du système d'information -

Date de mise en ligne : dimanche 12 mars 2006

Sommaire

- Complexité en expansion, risques multipliés
- Règles de conduite
- Secret professionnel
- Mots de passe
- Proposition de charte
- Préambule
- Définitions
- Responsabilités du comité de coordination SSI
- Surveillance et audit
- Contrôle d'accès
- Vérification
- Responsabilités de l'administrateur de système et de réseau
- Enregistrement des incidents de sécurité
- Journalisation et archivage
- Examen des journaux
- Dérogations aux règles SSI
- Audits périodiques
- Mise en œuvre et litiges
- Veille SSI
- Attitude à l'égard des violations de la loi
- Attitude à l'égard des violations des règles SSI

Complexité en expansion, risques multipliés

La multiplication de questions de plus en plus complexes liées à la sécurité des systèmes et des réseaux, l'imbrication de plus en plus intime des aspects techniques et juridiques de ces questions et le risque accru de conséquences judiciaires en cas d'erreur incitent à la rédaction, au sein de chaque entreprise ou organisation, d'une charte de l'administrateur de système et de réseau qui rappelle les devoirs, les pouvoirs et les droits des ingénieurs et des techniciens qui administrent la sécurité des réseaux, des ordinateurs et en fin de compte du système d'information.

En effet la situation de cet administrateur de système et de réseau le confronte à un certain nombre de paradoxes : par exemple, il doit configurer son système d'acheminement de messagerie électronique (Mail Transfer Agent, MTA, ou passerelle de messagerie) de façon à tenir un journal de tous les messages émis et reçus par le point d'accès à l'Internet dont il est responsable, c'est une obligation légale. Mais s'il oublie de détruire ces journaux à l'issue d'un délai maximal d'un an, il enfreint une autre obligation légale.

Cette activité d'administration de la passerelle de messagerie de l'entreprise lui permet de détecter les usages contraires à la loi qui pourraient en être faits par des employés indélicats, dont les exemples les plus courants sont, non limitativement :

– envoi de messages ou abonnement à des listes de diffusion susceptibles de tomber sous le coup des lois qui

répriment le racisme et la xénophobie, la pédophilie ou le trafic d'êtres humains ;
– communication à des tiers d'informations couvertes par le secret professionnel, qui constituent le patrimoine intellectuel de l'entreprise, et dont la divulgation à des concurrents est de nature à causer un préjudice certain ;
– infraction à la législation sur la propriété littéraire et artistique, lorsque les serveurs de l'entreprise sont utilisés pour télécharger ou, pire, redistribuer des oeuvres musicales ou cinématographiques couvertes par des droits d'auteur ;
– délit de presse, par l'ouverture de sites WWW ou de forums au contenu susceptible d'être attaqué au titre des lois sur la diffamation, le plagiat, etc.

La constatation de telles infractions lui fait devoir d'y mettre fin, mais dans les cas où les manifestations de ces actes ne sont pas publiques (cas du courrier électronique), s'il en fait état dans un rapport à la direction de l'entreprise, il s'expose à être condamné par un tribunal en vertu de la loi qui protège le secret de la correspondance. En effet, si la jurisprudence (arrêt du 17 décembre 2001 de la Cour d'Appel de Paris, « ESPCI », École Supérieure de Physique et Chimie industrielle) reconnaît que l'administrateur détient la possibilité technique de lire les contenus des messages, celui-ci n'est en revanche pas autorisé à les divulguer même à ses supérieurs hiérarchiques.

« Ainsi la délicate mission de l'administrateur sera de mettre fin au comportement frauduleux ou préjudiciable sans en informer son supérieur hiérarchique qui dispose pourtant de l'autorité et du pouvoir de décision », note Laurence Freyt-Caffin [1].

De façon plus générale, l'administrateur de système et de réseau a accès à toutes les données de l'entreprise et des utilisateurs qui stationnent ou circulent sur les machines et les réseaux dont il a la responsabilité : ce pouvoir le soumet en permanence à la tentation d'en abuser, même si ce n'est que pour simplifier sa tâche, ou rendre service aux utilisateurs, ou pour assurer le bon fonctionnement des infrastructures en question.

De façon nettement plus embarrassante, il peut recevoir de sa hiérarchie des injonctions contraires aux lois : il est alors placé devant le dilemme d'avoir à désobéir à ces injonctions, ce qui peut mettre en péril sa situation professionnelle, ou d'enfreindre la loi, ce qui risque de le mener devant un juge.

Règles de conduite

Secret professionnel

Le devoir de secret professionnel s'impose aux administrateurs ayant accès aux données personnelles des utilisateurs dans le cadre de leurs fonctions.

- Arrêt de la Chambre sociale de la Cour de cassation en date du 2 octobre 2001 : « Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. »
- Code du Travail, articles L432-2-1 : « Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci. Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant

un contrôle de l'activité des salariés. »

Mots de passe

J'emprunte ici à Patrick Chambet les idées qu'il a exprimées sur la liste de diffusion de l'Ossir[2] :

« - Non ! Les administrateurs ne doivent jamais connaître les mots de passe des utilisateurs.

– Pourquoi l'administrateur n'a-t-il pas besoin de connaître les mots de passe ?

– Un administrateur est, par définition, celui qui possède des privilèges élevés. En particulier, il peut effectuer toutes les tâches nécessaires en l'absence des utilisateurs, comme par exemple la prise de possession de fichiers, la modification des permissions d'accès à des ressources, etc... Pour cela, il n'a pas besoin et ne doit pas [commettre d'usurpation de personnalité] (se loger avec le login et le mot de passe de l'utilisateur).

S'il doit tout de même se résoudre à cela, l'utilisateur légitime devrait être présent (ce point devrait être débattu par les juristes de la liste, car le règlement intérieur de l'entreprise, la charte informatique, la politique de sécurité et les lois, décrets et jurisprudence entrent en jeu).

Il arrive que l'administrateur fasse tourner un craqueur de mots de passe pour vérifier la robustesse des mots de passe des utilisateurs. Mais dans ce cas, dès qu'un mot de passe est craqué, il doit demander immédiatement à l'utilisateur de le changer pour un mot de passe de robustesse au moins équivalente. Il ne le connaît donc plus.

– Pourquoi l'administrateur ne doit-il pas connaître les mots de passe ?

– Tout d'abord pour dégager sa responsabilité en cas d'activité délictueuse effectuée à l'aide d'un compte utilisateur particulier : l'utilisateur en question ne pourra plus dire que ce n'est pas lui, mais l'administrateur qui a envoyé tel [message électronique].

Ensuite pour le respect de la confidentialité des ressources utilisateurs (classifiées ou non), même si, par définition, un administrateur pourra toujours, à l'aide d'une action volontaire et avec un intention évidente (plaidable devant un juge si l'administrateur n'a pas reçu d'ordre explicite), accéder aux ressources en question.

D'un côté l'administrateur est protégé, de l'autre il devient plus facilement condamnable. »

Les injonctions hiérarchiques à violer le secret des mots de passe sont fréquentes, souvent pour des raisons en apparence excellentes : accéder aux données cruciales détenues par un utilisateur en vacances et inaccessible en est l'exemple typique. Il peut être très difficile de résister à une telle demande, et l'utilisateur à son retour peut détecter l'intrusion en consultant les journaux du système. Certes l'administrateur peut détruire ou modifier les éléments de journalisation relatifs à son action, mais cette altération même des journaux peut être détectée, quoique plus difficilement, et en cas de comparution devant un tribunal il aura ainsi considérablement aggravé sa faute. Si pour une raison ou pour une autre les relations entre le possesseur des données et son employeur ou l'administrateur sont conflictuelles, on voit toutes les conséquences fâcheuses que peut entraîner cet enchaînement de circonstances. Il convient donc d'éviter absolument de commettre de telles actions.

Proposition de charte

Préambule

La présente Charte de l'Administrateur de Système et de Réseau de l'INSIGU est destinée à déterminer les devoirs, les pouvoirs et les droits des ingénieurs et des techniciens qui administrent la sécurité des réseaux, des ordinateurs et du système d'information de l'INSIGU.

Cette Charte est promulguée en référence à la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSIGU (cf. section 8.1), qu'elle complète et dont elle est inséparable.

Définitions

Les entités de l'INSIGU, ses ressources informatiques, ses services Internet et les utilisateurs du Système d'Information qu'ils constituent sont définies ici comme dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSIGU (cf. section 8.1).

L'administrateur d'un système ou d'un réseau de l'INSIGU est toute personne, employée ou non par l'INSIGU, à laquelle a été confiée explicitement et par écrit, sous la forme d'une lettre de mission, d'un profil de poste annexé au contrat de travail ou d'un contrat de prestations de service, la responsabilité d'un système informatique, d'un réseau ou d'un sous-réseau administrés par une entité de l'INSIGU, ou de plusieurs de ces éléments. Une personne à qui a été conférée une telle responsabilité sera désignée dans la suite de ce document par le terme administrateur. L'ensemble des éléments sur lesquels s'exerce cette responsabilité constitue le périmètre d'activité de l'administrateur.

Le comité de coordination de sécurité du système d'information (SSI) est constitué de responsables chargés d'émettre des règles et des recommandations dans le domaine SSI, de prendre les mesures appropriées pour qu'elles soient mises en vigueur, et d'organiser les activités de formation, d'information et de sensibilisation de nature à améliorer les conditions de leur application. Les membres de ce comité de coordination sont le Responsable de Sécurité des Systèmes d'Information (RSSI) de l'INSIGU, le Responsable de la Sécurité Opérationnelle au sein du Département du Système d'Information (DSI) de l'INSIGU, et d'autres personnes désignées par le Directeur Général de l'INSIGU ou son représentant autorisé.

Les devoirs, les pouvoirs et les droits de l'administrateur, définis dans la présente Charte, constituent ensemble les responsabilités SSI de l'administrateur.

Les consignes du comité de coordination SSI s'imposent aux administrateurs de systèmes et de réseaux pour l'exercice de leurs responsabilités SSI dans leur périmètre d'activité.

Responsabilités du comité de coordination SSI

Surveillance et audit

Le comité de coordination SSI organise la surveillance et l'audit de toutes les activités des systèmes et de tous les trafics réseau sur les infrastructures administrées par l'INSIGU.

Pour ce faire, le comité de coordination SSI est habilité à donner des consignes de surveillance, de recueil d'information et d'audit aux administrateurs concernés.

Contrôle d'accès

Le comité de coordination SSI définit des règles de contrôle d'accès aux systèmes et aux réseaux conformes à la présente Charte et à la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSIGU.

Vérification

Le comité de coordination SSI et les administrateurs concernés sont habilités à entreprendre toutes actions appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies à l'article précédent, ainsi que pour détecter leurs vulnérabilités.

Responsabilités de l'administrateur de système et de réseau

Enregistrement des incidents de sécurité

L'administrateur conserve une trace écrite des incidents de sécurité survenus dans son périmètre d'activité. Cette trace doit comporter les indications de date et d'heure des événements considérés, et une description de ces événements.

Journalisation et archivage

L'administrateur active sur les systèmes dont il a la responsabilité les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements qui pourraient constituer un incident de sécurité, ou qui pourraient faire l'objet d'une commission rogatoire émise par les autorités judiciaires. Il archive les données ainsi recueillies dans des conditions propres à en assurer l'intégrité, la disponibilité, l'authenticité et la confidentialité.

Il mène cette activité de journalisation et d'archivage dans des conditions qui garantissent le respect des lois et des règlements relatifs aux libertés publiques et privées, au secret des correspondances, au droit d'accès à l'information, et il veille notamment à détruire tous les journaux qui comportent des données nominatives à l'expiration d'un délai qui ne peut excéder un an, ou le délai légal à la date considérée.

Parmi les textes législatifs et réglementaires qui s'appliquent à cette activité, il convient d'accorder une attention particulière à la Norme simplifiée nÂ°46 de la Commission Nationale Informatique et Libertés, « destinée à simplifier l'obligation de déclaration des traitements mis en oeuvre par les organismes publics et privés pour la gestion de leurs personnels ».

Examen des journaux

L'administrateur examine régulièrement les journaux mentionnés à l'article ci-dessus.

Dérogations aux règles SSI

Les règles SSI mentionnées dans la présente Charte, dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSIGU, ou édictées par le RSSI de l'INSIGU, par le Responsable de la Sécutité Opérationnelle au sein du DSI de l'INSIGU ou par le comité de coordination SSI s'imposent à tous les utilisateurs des Systèmes d'Information de l'INSIGU, qu'ils soient on non des employés de l'INSIGU. Les administrateurs de systèmes et de réseaux de l'INSIGU ont pour mission de les mettre en oeuvre et de les faire respecter dans leur périmètre d'activité.

Les responsables d'entités qui voudraient passer outre ces règles SSI, ou entreprendre des actions qui dérogeraient à ces règles, doivent remettre à l'administrateur responsable des infrastructures concernées un document écrit et signé par lequel il assume explicitement la responsabilité de cette dérogation, des risques qui en découlent, et de leurs conséquences.

Les utilisateurs qui ne seraient pas responsables d'entités et qui voudraient bénéficier de telles dérogations doivent obtenir qu'elles soient endossées par leur responsable d'entité, dans les conditions indiquées à l'alinéa précédent.

Identification des utilisateurs et contrôles d'accès
Dans leur périmètre d'activité, les administrateurs responsables sont seuls habilités à mettre en place et à administrer les systèmes d'identification et d'authentification des utilisateurs conformes aux directives du comité de coordination SSI. Il en va de même pour les dispositifs de contrôle d'accès aux systèmes, aux réseaux et aux données.

Sauf exception formulée par un document écrit signé d'un responsable d'entité, seuls l'administrateur local et ses collaborateurs immédiats possèdent les droits d'administrateur sur les postes de travail des utilisateurs des SI de l'INSIGU.

Audits périodiques

Les administrateurs procèdent deux fois par an à un audit des comptes des utilisateurs et des droits d'accès associés, pour vérifier leur validité et leur exactitude.

Mise en œuvre et litiges

Rapport des violations des règles SSI
Pour toute violation des règles SSI qu'il est amené à constater, l'administrateur établit un rapport écrit destiné au comité de coordination SSI et à ses responsables hiérarchiques.

Veille SSI

Les administrateurs exercent régulièrement une activité de veille scientifique et technologique dans le domaine SSI. Ils sont abonnés aux listes de diffusion qui publient les découvertes de vulnérabilités. Ils participent notamment aux activités de formation, d'information et de sensibilisation entreprises par le comité de coordination SSI.

Attitude à l'égard des violations de la loi

Lorsque l'administrateur constate des violations de la loi dans son périmètre d'activité, il en fait rapport au comité de coordination SSI et à ses responsables hiérarchiques, qui prendront les mesures adéquates afin de coordonner leurs actions avec les autorités judiciaires.

Attitude à l'égard des violations des règles SSI

La direction de l'INSIGU, ou son représentant qualifié, peut révoquer le compte et les droits d'accès au réseau et aux données d'un utilisateur qui aurait violé les règles SSI mentionnées dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSIGU.

---

[1] Laurence Freyt-Caffin. « L'administrateur réseau, un voltigeur sans filet ». *5èmes journées réseau JRES*, 2003. En ligne ici : http://2003.jres.org/actes/paper.130.pdf.