Document politique de sécurité : Cas de l'ENSIAS

Contexte

La modernisation des grandes écoles d'ingénieurs repose sur la possibilité, pour les étudiants, l'administration et le corps professoral, de s'échanger des informations de façon rapide et sécuritaire. C'est dans cette optique que l'ENSIAS a mis en place un système d'information muni d'un réseau permettant d'assurer la disponibilité de l'information pour tout le monde. Dans la perspective d'un volume accru d'échanges d'information et afin de s'assurer du respect des lois, règlements et normes gouvernementales en matière de sécurité de l'information, le Ministère a élaboré un Cadre global de la sécurité des actifs informationnels. La volonté du Ministère est de mettre en place, au cours des trois (3) années qui suivent, l'ensemble des mesures prévues au Cadre global de sécurité.
L'établissement reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. L'établissement reconnaît détenir, en outre, des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative ou économique. De plus, plusieurs lois et directives encadrent et régissent l'utilisation de l'information.
L'établissement est assujetti à ces lois et doit s'assurer du respect de celles-ci. (Note : il serait possible d'indiquer les principales lois et directives, nous vous référons à l'annexe H Fondements juridiques pour une liste complète).
En conséquence, l'établissement met en place la présente politique de sécurité de l'information qui oriente et détermine l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information.
D'autre part, l'ENSIAS est supposé leader au niveau national et international dans le marché du B2C, puisqu'elle dispose d'une plate-forme de e-commerce developpée et maintenue localement, qu'elle commercialise auprès de clients nationaux et internationaux.

1. Messagerie (Liste de diffusion) de l'ENSIAS (palte-forme um5s)

L'usage de liste de diffusion est autorisé sous les conditions suivantes :

1. Toutes listes de diffusion comprenant plus de 100 destinataires doit avoir :

- l'aval du doyen (ou d'un représentant) si l'ensemble des destinataires comprend des étudiants qui n'appartiennent pas au groupe des administrateurs de la liste de diffusion,
- l'aval du vice-président de l'université ou du service des ressources humaines si l'ensemble des destinataires comprend des employés qui n'appartiennent pas au groupe des administrateurs de la liste de diffusion,

2. le contenu du message doit être inclus dans le message lui-même et pas en pièce jointe dans la mesure du possible,

3. le message doit préférentiellement contenir des liens plutôt que des pièces jointes afin d'éviter d'augmenter la taille du message.

L’usage des emails est interdit dans les contextes suivants (liste non exhaustive) :

- l’objectif du message envoyé viole une loi fédérale,
- le message est à caractère commercial,
- l’identité de l’émetteur n’apparaît pas,
- l’envoi de masse congestionnant le réseau,
- la diffusion de messages inappropriés à des listes ou des individus,
- attribution d’une priorité « élevée » à un message envoyée sur une liste de diffusion.

2. Politique de sécurité du serveur web de la plateforme e commerce (ISO 17799:2005 10.9) :

2.1 Administration de la plateforme :

- **Administration local (ISO 17799:2005 11.4):**

Il est recommandé d’administrer un serveur localement, c’est à dire à partir de sa console.
Pour ces activités, l’administrateur utilisera ponctuellement un compte dédié avec les privilèges adéquats.
Pour les tâches ne nécessitant pas de tels privilèges, l’administrateur prendra soin d’utiliser un autre compte, avec des droits restreints.

- **Administration distante :**

Néanmoins, si une administration distante du serveur est requise, elle ne devrait pas pouvoir être réalisée depuis n’importe quel poste du réseau interne. Il est donc nécessaire de limiter cette fonctionnalité aux seuls postes des administrateurs, en particulier au niveau de leur adresse IP.
Toutefois, l’utilisation de stations dans un rôle d’administration impose que le niveau de sécurisation de la station d’administration à distance soit au moins équivalent à celui du serveur (sécurité physique et logique). S’il est nécessaire de se connecter à travers le réseau sur le serveur, il est préférable d’utiliser des outils d’administration chiffrés, fournis avec le système ou tiers en raison des possibilités d’écoute.

2.2 Gestion des utilisateurs (ISO 17799:2005 11.2) :

Dans notre cas on aura besoin d’un moyen fort de confidentialité ET on aura aussi besoin d’identification fort du client, pour ceci on doit mettre en place un certificat sur le serveur Web et exiger l’utilisation de certificats personnels par le client. Bien entendu il faudra aussi contrôler les certificats utilisateurs, définir ceux accepter, les procédures de mise à jour etc. Cette solution est la plus lourde mais aussi la plus sûre en cas de besoin fort de confidentialité et identification. Cela implique la mise en place d’une solution d’IGC (PKI).

2.2 Contrôle du contenu des champs de formulaire (ISO 27001 – A.10.4):

Une attaque courante sur les serveurs ayant des formulaires réside dans l'envoi de code malicieux au travers des champs de formulaires, ceci afin de déstabiliser le système, injecter du code dans la base de données ou prendre le contrôle de la machine. Il est donc important de sensibiliser des développeurs du site Web au contrôle des différents champs retournés par l'utilisateur au travers des formulaires. Il est primordial de traiter tous les champs retournés par le visiteur avant de les utiliser dans un quelconque procédé. Il sera profitable de mettre en place sur le serveur un module dédié au contrôle des caractères utilisés. Le seul champ pour lequel certains caractères spéciaux peuvent sembler nécessaires est le champ de mot de passe.

3. Sécurité des actifs de l'établissement de l'ENSIAS (ISO 27001 A.7 et A.9.2)

a) Toute personne au sein de l'ENSIAS ayant accès aux actifs informationnels* assume des responsabilités spécifiques en matière de sécurité et est redevable de ses actions auprès du directeur de l'Ecole.

b) La mise en œuvre et la gestion de la sécurité reposent sur une approche globale et intégrée. Cette approche tient compte des aspects humains, organisationnels, financiers, juridiques et techniques, et demande, à cet égard, la mise en place d'un ensemble de mesures coordonnées.

c) Les mesures de protection, de prévention, de détection, d'assurance et de correction doivent permettre d'assurer la confidentialité, l'intégrité, la disponibilité, l'authentification et l'irrévocabilité des actifs informationnels de même que la continuité des activités. Elles doivent notamment empêcher les accidents, l'erreur, la malveillance ou la destruction d'information sans autorisation.

d) Les mesures de protection des actifs informationnels doivent permettre de respecter les prescriptions du Cadre global de gestion des actifs informationnels appartenant aux écoles d'ingénieurs – Volet sur la sécurité, de même que les lois existantes en matière d'accès, de diffusion et de transmission d'information, et les obligations contractuelles de l'établissement de même que l'application des règles de gestion interne.

e) Les actifs informationnels de l'ENSIAS doivent faire l'objet d'une identification et d'une classification.

f) Une évaluation périodique des risques et des mesures de protection des actifs informationnels doit être effectuée afin d'obtenir l'assurance qu'il y a adéquation entre les risques, les menaces et les mesures de protections déployées.

g) La gestion de la sécurité de l'information doit être incluse et appliquée tout au long du processus menant à l'acquisition, au développement, à l'utilisation, au remplacement ou la destruction d'un actif informationnel par ou pour l'établissement.

h) Un programme continu de sensibilisation et de formation à la sécurité informatique doit être mis en place à l'intention du personnel et des Etudiants de l'ENSIAS.

i) L'accès aux renseignements personnels des utilisateurs par le personnel de l'ENSIASdoit être autorisé et contrôlé. Chaque système doit prévoir des droits d'accès différents selon les catégories de personnel.(Administration , Etudiants, Etrangers)

j) Les renseignements personnels ne doivent être utilisés et ne servir qu'aux fins pour lesquels ils ont été recueillis ou obtenus.

k) Le principe du « droit d'accès minimal » est appliqué en tout temps lors de l'attribution d'accès aux informations. Les accès aux actifs informationnels sont attribués à l'utilisateur autorisé en fonction de ce qui lui est strictement nécessaire pour l'exécution de ses tâches.

l) Les ententes et contrats dont l'établissement fait partie doivent contenir des dispositions garantissant le respect des exigences en matière de sécurité et de protection de l'information.

*Actif Informationnel : Ordinateurs de bureau (Dans les salles de TP, l'Administration, la Bibliothéque), Serveurs (Centre de Calcul), les équipements réseaux (Routeurs, Switchs, Hub, câblages).