Règles de sécurisation d'un site Web sur l'Université Lille 1

L'objet de ce document est de préciser les règles de sécurité qui s'imposent à tous les responsables et webmestres de sites Web de l'Université.

Tout "intervenant" sur le réseau de Lille1 est un utilisateur des ressources informatiques de Lille1. Il est déjà soumis au Règlement d'usage du Système d'Information (cf. http://cri.univ-lille1.fr/Documents-formulaires/Charte-Informatique/) .

Règles techniques

Les responsables d'un site s'engagent à assurer la sécurité du site, autrement dit à mettre en œuvre pendant toute sa durée de vie les mesures permettant de fournir la bonne information, au moment désiré, uniquement à ceux qui en ont besoin.

Une liste très complète des mesures techniques et organisationnelles de sécurisation d'un site WEB a été éditée par l'Agence Nationale de la Sécurité des Système d'Information (ANSSI). Cette liste est disponible à l'adresse suivante :

http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf

Nous encourageons vivement les responsables d'un site à consulter ce document et à mettre en oeuvre les mesures qui les concernent. Le simple respect de ses mesures permettant de réduire considérablement les risques de compromission.

Parmis les mesures prioritaires, vous trouverez notamment :

- maj du système d'exploitation (ne concerne pas les sites hébergés au CRI)
- maj des logiciels type CMS (ne concerne pas les sites hébergés sur CMS du CRI)
- Les composants applicatifs employés doivent être limités au strict nécessaire
- Les composants applicatifs employés doivent être recensés et maintenus à jour
- L'administration d'un site web doit se faire via des protocoles sécurisés
- L'accès aux mécanismes d'administration doit être restreint aux seuls postes d'administration autorisés
- Les administrateurs doivent être authentifiés de manière sûre
- Les fichiers pouvant être servis aux clients doivent être limités au strict nécessaire
- Les droits sur la base de données doivent être gérés finement pour mettre en œuvre le principe de moindre privilège
- Les requêtes adressées à la base de données doivent être faites au moyen de requêtes préparées fortement typées ou par l'intermédiaire d'une couche d'abstraction assurant le contrôle des paramètres. Dans les (rares) cas où cette approche serait impossible, il convient d'apporter un soin particulier à s'assurer que les données manipulées ne comportent pas de caractères spéciaux (au sens du SGBD) sans échappement et ont bien la forme attendue
- Limiter les renseignements fournis sur le fonctionnement technique du site web.
- Les traitements doivent tous être faits du côté du serveur. Les entrées en provenance des clients ne doivent pas être considérées comme fiables et par conséquent, aucune vérification

ne doit être déléguée aux clients

- Favoriser les redirections statiques plutôt que d'employer des redirections controlées par des données externes
  Pour les redirections dynamiques, adopter un fonctionnement en liste blanche en vérifiant que les URL visées soient légitimes
- L'inclusion de fichiers dont le nom ou le chemin d'accès dépend d'une donnée externe ne doit pas être employée
- Il faut recourir à chaque fois que c'est possible au protocole HTTPS dès lors que l'on associe une session à des privilèges particuliers
- Les mots de passe ne doivent pas être stockés en clair mais dans une forme transformée par une fonction cryptographique non réversible
- Limiter les sites WEB dynamiques

En cas de non respect des mesures ci-dessus et si le site est compromis, le CRI, qui a pour mission d'assurer un niveau de sécurité adéquat sur le réseau de l'université, sera dans l'obligation de fermer le site.

Un site ne sera ré-ouvert qu'après un test de sécurité validé par les services du Cri et un accord du vice président TIC.