Les axes stratégiques de développement des établissements et la sécurité de l'information

Alain BRILLARD
Ancien Président de l'Université de Mulhouse
AMUE – 28 novembre 2012

Contexte et historique

- UHA = université pluridisciplinaire hors santé
- 8000 étudiants
- 500 enseignants et chercheurs, 450 personnels administratifs, plusieurs centaines d'enseignants vacataires
- 2 villes, 5 campus, 8 composantes (dont 4 dérogatoires)
- Passage aux RCE en 2009 (première vague)

Des risques (1)

- Antérieurement à 2007 : un Centre de Ressources Informatiques, avec un éclatement des ressources humaines et des installations entre le niveau central et les composantes
- Système d'information : « patchwork » entre des applications COCKTAIL (JEFYCO, MANGUE…), AMUE (APOGEE) et autres (ADE…)
- Difficultés cycliques de recruter des ressources humaines en « informatique »
- Adoption d'un schéma directeur informatique le 30 avril 2008, comportant un volet sécurité

Des risques (2)

- Hébergement sur les serveurs de l'université de sites web de partenaires (un lycée (jusqu'à peu), le CCSTI haut-rhinois Nef des sciences)
- Convention avec le CROUS pour l'accès des étudiants en cités universitaires au réseau
- Activités de recherche parfois à haut risque
- Enseignement à Distance et accès distant aux bases de données + publications (SCD)
- Messageries « privées »

Des risques (3)

- Forte couverture wifi (dans le cadre de l'Université Numérique en Région Alsace)
- Déploiement d'EDUROAM
- Activités classiques de conférences, colloques… et parfois missions dans des pays jugés « à risque »
- Quelques bornes wifi « pirates », liées à des activités de formation et de recherche

Eléments du rapport d'audit RCE (1)

- *Clarifier les niveaux et modalités de pilotage du système d'information entre l'université et ses diverses composantes*
- *Valider et mettre en œuvre le projet de schéma directeur informatique*
- *Sécuriser la salle machine du CRI*
- *Créer un entrepôt de données exploitables*

Eléments du rapport d'audit RCE (2)

- *Développer l'interopérabilité des applications*
- *Introduire et installer un management participatif au service d'objectifs partagés par le niveau central comme par les composantes*
- *Garantir la fiabilité de l'information et élaborer certains critères et indicateurs*
- *Assurer le contrôle de la qualité des données et la mise à jour régulière du système d'information*

Politique SSI

Pas de réelle politique SSI, au sens d'un texte partagé et validé, mais :

- Nomination d'un RSSI depuis 10 ans (rapport annuel)
- Université plus que sensibilisée aux risques dans différents domaines (formations et recherches sur la gestion des risques)
- Incrémentation régulière des parades

Eléments de politique SSI (1)

- Réorganisation de la Direction Informatique
- Déménagement des salles serveurs dans des locaux plus sécurisés
- Sécurisation des serveurs (installation des sites web de manière centralisée sur une DMZ)
- Mise en place d'un serveur captif pour le wifi (utilisation de protocoles sécurisés)

Eléments de politique SSI (2)

- Accès VPN chiffré (EDUROAM en connexion chiffrée 802.1X)
- Sauvegarde des données
- Déploiement d'antivirus
- Annuaire LDAP centralisé
- Politique de sensibilisation des chercheurs et de tous les acteurs (classement de certains laboratoires en zones à risque)

Eléments de politique SSI (3)

- Convention avec le CROUS pour l'accès des étudiants au réseau informatique
- Conventions avec les partenaires hébergés
- Procédure de changement de mots de passe
- Sécurisation des données (personnels, étudiants)
- Simplification de l'organisation du réseau informatique alsacien
- Politique de mots de passe (changements, tests de niveau de « résistance »…)

A faire

- Nettoyage de l'annuaire LDAP
- Bornes wifi « pirates » à encadrer
- Formations sur la sécurité du SI à développer (et motiver les collègues pour y participer)

et…

- Formaliser la politique SSI (mettre en place les structures…)

Conclusion

- Il sera important d'analyser les risques résiduels, en préparation à la mise en œuvre d'une véritable politique SSI
- Augmenter les parades, compte tenu des « progrès » effectués lors des attaques
- Toujours sensibiliser les acteurs sur les risques encourus