Journée de Formation Technique du 1 octobre 2013

L'approche de la sécurité pour un DSI

L'apport de l'expert judiciaire

Jean-Pascal de La FAYE
43 rue Blanche
75009 PARIS
pdelafaye@hotmail.fr
Tél : 06 87 70 92 51

La Sécurité pour un DSI

Pour un DSI, la gestion de la Sécurité :

- Est une préoccupation permanente
- Concerne tous les domaines : processus, systèmes d'information, automatismes, Bureautique et Télécommunications, …
- Est abordée sous l'angle de la Gestion des Risques
- Fait partie de la Gouvernance Informatique, et se traduit concrètement par des actions, des infrastructures, des normes, des procédures, des outils, des contrôles, des tests, des audits, des ressources dédiées, …

L'approche multi-domaines de la Sécurité

- **Sécurité Physique des infrastructures** :

  Salles blindées et étanches , redondance des équipements et des sources d'énergie, onduleurs, extinction incendie, capteurs d'humidité et de température, surveillance, contrôles d'accès, ….

- **Sécurité et Intégrité des Données et des Référentiels** :

  Procédures, contrôles, règles de gestion, infrastructures de stockage redondantes, Dictionnaire standard des Données, …

- **Sécurité de fonctionnement – Continuité de Service**

  Procédures d'exploitation, sauvegardes, back-up, sites de secours, DRP (Desaster Recovery Plan) et PCA (Plan de Continuité d'Activité), procédures de gestion des incidents , ….

- **Sécurité Logique et Applicative :**

  Outils de monitoring d'exploitation, contrôles programmés, points de reprise, outils d'EAI (Entreprise Application Integration) et d'ESB (Entreprise Service Bus), contrôles croisés, Core Models applicatifs, ….

- **Sécurité d'accès aux systèmes aux données :**

  Gestion des Logins et mots de passe, procédures, sécurisation des VPN, politique de cryptage, surveillance de l'utilisation et procédures de Data Leak Prevention, gestion centralisée des Fire-Walls, …

- **Sécurité des outils bureautiques** :

  Anti-virus, mises à jour régulières des logiciels, équipes de support, câbles anti-vol, cryptage des données, contrôles à distance, marquages, outils de MDM (Mobile Devices Management), …

- **Sécurité Juridique** :

  Audits de conformité, CNIL, procédures de conservation des données légales, veille règlementaire, contrôles de licences, revue des contrats, sensibilisation juridique, Protection contre les délits de marchandage et de prêt de main d'œuvre illicite, procédures d'achat, BCR (Binding Corporate Rules), engagement de confidentialités, chartes, ….

- **Sécurité des Ressources et des actifs :**

  Dépendance de Prestataires ou de collaborateurs clés, pérennité des prestataires et des éditeurs, obsolescence des équipements et des logiciels, anticipation des compétences à recruter, ….

Domaines plus difficiles à maîtriser

- **Sécurité stratégique à moyen - long terme :**

  Adéquation des systèmes aux besoins de l'entreprise :
  Plan d'Urbanisme applicatif et technique, processus d'Alignement
  Stratégique, Suivi et prévision des volumes et performances,
  veille technologique, modernisation continue des systèmes et infrastructures, ….

- **Sécurité d'utilisation :**

  Prévention des risques liés à la négligence ou aux erreurs des utilisateurs,
  et à la malveillance externe et interne :
  Procédures et outils de contrôle, gestion des accès, actions de formations
  et de sensibilisation, …..

Domaines particuliers de l'expert judiciaire

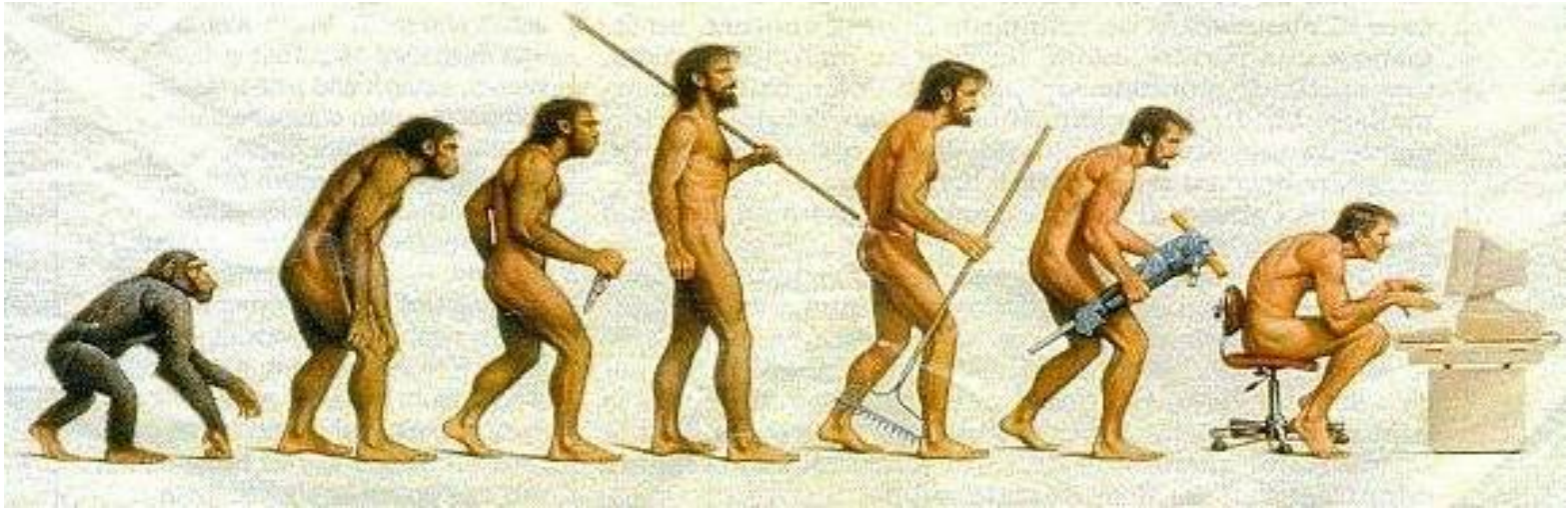
- **Gouvernance de la Sécurité**

  Normes COBIT , COSO , procédures de gestion des risques, Normes et Standards de Sécurité des systèmes, audits et expertises techniques, ….

- **Sécurité des projets et changements** :

  Bonnes pratiques de gestion de projet, séparation et responsabilités des MOA et MOE, cycle en V, adéquation des moyens, structures et comités, documentation (cahier des charges, spécifications fonctionnelles, dossier d'architecture, cahier de recette, jeux d'essais, ….) , PAQ Plan d'Assurance Qualité formalisant les responsabilités (RACI), processus d'arbitrage, de validation, de test , de recette, …, gestion des risques projets, ….

Une grande partie des conflits informatiques sont la conséquence du non respects des bonnes pratiques et règles de prudence et de sécurité par les parties.



Merci de votre attention