Risques du métier

C. BENSARI

Introduction

- Il existe un nombre important de risques dont les conséquences s'appliquent à des domaines très différents dans l'entreprise : les métiers, les relations clients, partenaires ..
- Les risques liés au numérique surviennent lors du passage du système d'information (SI*) de l'entreprise au numérique
- Il existe différentes catégories de risques pour l'entreprise (RH, Rapports humains, stratégies, contrôle du SI, périphériques, ..)
- Pour maitriser ces risques, chaque acteur de l'entreprise doit être sensibilisé afin d'avoir le bon comportement dans certaines situations au sein de l'entreprise

*** : Un système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information**

Les bons comportements à adopter

- Ne pas divulguer des informations sensibles (confidentielles) :
  - Information connue uniquement de la direction de l'entreprise
  - Information qui touche les secrets et stratégies
  - Information qui mettra en difficulté l'entreprise
- Etre vigilant vis-à-vis des mails reçus en provenance de sites connus ou inconnus. Rappel des types de menaces :
  - Spam : courriers indésirables afin de saturer le serveur
  - Malware : logiciel malveillant malveillant (exemple attaque de 2012 aux USA avec un logiciel d'écoute de saisi clavier sur des sites de banques (5.7 millions de $ de pertes))
  - Phishing : un mail provenant de sites connus par l'utilisateur avec un lien qui méne vers une page de saisie d'informations sensibles ou un lien de téléchargement d'un logiciel malveillant qui vole des données

Les bons comportements à adopter

- Eviter l'utilisation de disque de stockage privé (USB, ..)
- Eviter de consulter des sites potentiellement dangereux et faire attention aux cliques sur des liens dans des forums (consultation ou téléchargement)
- Prendre soins du matériel informatique fourni par l'entreprise (pas d'utilisation personnelle, pas de liaison avec internet à l'extérieur du réseau de l'entreprise et ne pas laisser le matériel à la portée de tous)
- Ne jamais fournir ses mots de passe et veiller à bien les sauvegardé dans un endroit sure