Règle n° 5 : S'assurer de la prise en compte de la sécurité dans les projets

Les approches de sécurité actuelles sont remises en cause par les nouvelles les technologies numériques, notamment avec l'apparition des réseaux sociaux, des applications mobiles et des objets connectés.
Les nouvelles approches de sécurité des SI s'appuient sur le fait que chaque composant du SI doit être résistant aux attaques. La prise en compte de cette démarche doit donc se faire au sein des projets de mise en œuvre des nouveaux usages puis de leur maintien en conditions opérationnelles et de leurs évolutions.

- **Analyser** et **évaluer** les risques liés à la solution concernée par le projet :
  - Principales menaces et vulnérabilités
  - Cartographie des risques
  - Niveau de risque et impacts associés
  - Mesures de réduction des risques, plan d'actions et budget associé
  - Indicateurs de suivi des actions de maîtrise des risques).

- **Définir** les Bonnes Pratiques de Sécurité pour l'élaboration des composants d'un SI et les normes à appliquer (ISO 27002) :
  - Robustesse des plateformes techniques (développement, test, production)
  - Qualité du code développé
  - Intégration des mécanismes de sécurité (authentification, confinement, cryptage, …)
  - Tests de vulnérabilité, ...

- **Veiller** à leur mise en œuvre et à leur respects
  - Sensibilisation, formation de l'équipe (y compris des prestataires)
  - Vérification des pratiques appliquées par les sous-traitants
  - Audit régulier par un Prestataire d'Audit de la Sécurité des SI (qualifié PASSI) sur les différents volets du projet : architecture, configuration, code source, tests d'intrusion, organisation, …

- **Prendre** des mesures préventives
  - Risques de cyber sécurité couverts par votre assurance et celle de vos prestataires
  - Veille sécurité sur les technologies utilisées dans les projets

Le **manuel de Cyber Sécurité** dans l'entreprise devient aussi important que le Manuel Qualité.

Faits

Recrudescence des cyberattaques contre les entreprises : Dans la zone EMEA, plus d'un tiers d'entre elles s'attendent à en être victimes dans les 3 prochains mois (Source : étude cabinet Vanson Bourne)

Frein au déploiement d'usages numériques innovants : 87 % des DSI estiment que ces nouveaux usages introduisent des vulnérabilités potentielles (Source : étude cabinet Vanson Bourne)

Clés de cryptage et certificats numériques dérobés
Ce type de vol, très lucratif pour les pirates, représentent un menace très importante pour la sécurité du SI des entreprises

Evolution des Ransomware : les pirates neutralisent d'abord les sauvegardes avant de déclencher le chiffrement des données de l'entreprise pour exiger une rançon

Résultats attendus

Valorisation de la démarche et des moyens de Cyber Sécurité dans le budget des projets numériques

Rédaction d'un Manuel de Cyber Sécurité

Démarche Cyber Sécurité appliquée à chaque projet

Audit régulier par des prestataires qualifiés PASSI

Assurance Cyber Sécurité