Club de la sécurité de l'information français

CLUSIF

Les coûts d'une cyber-crise

Gurvan QUENET, CLUSIR Aquitaine
Animateur au sein de la Cellule d'Animation

Des exemples récents

- Sony PSN : 172 M$
  - Mais une estimation prenant en compte les coûts indirects évoque 2 Milliards de Dollars
- Maersk : 400 M€ direct ; 1,5 Milliards indirect
- FedEx-TNT : 300 M$
- Saint Gobain : 250 M€ dont 220 M€ en perte de revenus
- Société de l'agro alimentaire : 10 M€

Des coûts mesurables

- Perte de production, d'exploitation, arrêt du SI / manque à gagner
- Coûts de mise en conformité, non respect de la législation (amendes)
- Coûts de justice (dommages et intérêts)
- Coûts contractuels / commerciaux
- Coûts de la remédiation et reconstruction IT
  - Sur le plan technique IT et SSI (expertise)
  - Organisationnel et gouvernance à repenser, au pire à définir !
  - Humain (sensibilisation / responsabilisation, compétences, …)

Des coûts difficilement mesurables

- Perte de confiance des fournisseurs et sous-traitants
- Perte de confiance des partenaires (financiers)
- Perte de confiance des clients
- Dégradation de l'image et réputation de l'entreprise (durée ?)
- Coûts sociaux, chômage technique, perte de poste
- Poursuites pénales (court ou moyen terme)

Des coûts complémentaires à prévoir

- Le RGPD
  - Sanctions de 4% du chiffre d'affaire mondial ou
  - Coût de notification aux tiers (violation de données) et indemnisations des clients (classe action…), ex : BtoC
  - Refonte du design du produit/service ou module défaillant, cible de l'attaque (ex : voiture connectée)

Objectif de la gestion de crise

- Évaluer la criticité de l'évènement
- Définir un plan d'action pour :
  - *Limiter les impacts métiers, financiers, juridiques*
- Maîtriser l'information tout au long de la crise (Réseaux sociaux à intégrer)
- Maîtriser la communication (à chaud) pour rassurer les salariés, les clients et partenaires
- Collecter les informations pour une communication (à froid) post-crise (anticipation des litiges potentiels, recours, etc.) pour un retour en mode nominal rapide
- Capitaliser sur l'historique post-crise et des incidents précédents (amélioration continue)

Pour

- **Maintenir les coûts directs ou indirects dans une enveloppe financière acceptable**

Comment limiter le coût d'une crise

- Anticiper en connaissant ses points de fragilité
- Analyse et traitement du risque
  - Mise en place de mesures de réduction du risques
  - Mise en place d'une cellule de gestion de la crise
  - Mise en place d'une communication maitrisée
  - Transférer le risque auprès d'une cyber assurance (indemnisation plafonnée et ne couvre pas tout)
- Acculturation digital / cyber sécurité
- S'inspirer des plans déjà mis en place (sanitaire/CHSCT, plan de secours usine, etc.)