Simulation de crise

La cyber attaque d’un cabinet d’avocat

side quest

Mise en situation : l’avant

- Un cabinet d’avocat de taille moyenne : 5 - 10 personnes
- Absence d’assurance spécifique
- Absence de sensibilisation à la gestion de crise (pas de procédure établie)
- Conformité RGPD “basique”
- Absence d’outils techniques très sécurisés (chiffrement, sauvegardes automatiques)

side quest

La crise : Un rançongiciel vient bloquer le cabinet

- Définition du Ransomware ?
- Description du mode opératoire habituel

side quest

L’impact sur le cabinet :

- Le cabinet ne peut pas ouvrir
- L’ensemble des logiciels sont bloqués
- Le cabinet ne peut pas opérer
- Fuite probable de données personnelles
- Possible atteinte à la confidentialité des relations client / avocat : exemples

Comment réagir ?

side quest

La réaction

- Une cellule de crise ?
- La continuité des activités ?
- La question de la sauvegarde de la preuve
- Les problématiques concernant la communication
- Porter plainte? Prévenir les autorités ?
- Revoir les contrats ?
- Prévenir les clients?
- Prévenir le dommage réputationnel ?
- Question de la conformité RGPD ?
- Faut-il ou non payer le ransomware?

side quest

Après la crise

L’importance du retour d’expérience

Processus d’amélioration continue

side quest

En définitive

- L’importance d’une préparation en amont
- En matière cyber des mesure d’hygiène simples (mots de passes, gestion des droits, chiffrement, formation …)
- L’importance d’une conformité RGPD
- Tout faire pour protéger sa réputation

side quest