PLAN DE CONTINUITE ET DE REPRISE D'ACTIVITE

RESUME
Nous verrons dans cette procédure un exemple de plan de continuité et de reprise d'activité informatique.

Théo MARTIN
SIO23

Plans de continuité et de reprise informatique

I) Particulier

Pour un particulier, les menaces et les risques informatiques sont nombreux.

Tout d'abord nous allons identifier les différents types de menaces :

- Menaces humaines :
  - Cyber-attaque, virus
  - Perte/vol du matériel (ordinateur, disque dur, téléphone portable)
  - Panne du matériel (défaut de fabrication ou autre)
- Menaces naturelles :
  - Dégât des eaux
  - Incendie

Après avoir défini les menaces, nous allons établir deux plans, un plan de continuité informatique et un plan de reprise informatique.

- Plan de Continuité Informatique (PCI) :
  - Mesures de protection :
    - Pour éviter la perte de données, le particulier pourrait tout sauvegarder sur le Cloud (via Google Drive ou encore OneDrive)
    - Il pourrait installer un antivirus et souscrire à un abonnement pour avoir une sécurisation plus approfondie
    - Garder une copie dans un lieu différent pour prévenir les dégâts physiques
    - Souscrire à une extension de garantie pour réparer le matériel
- Plan de Reprise Informatique (PRI) :
  - Mesures de protection :
    - Remplacer/réparer le matériel défectueux
    - Utiliser une des sauvegardes

II) Entreprise

Pour une entreprise le PCI/PRI est légèrement différent, en effet les risques sont plus importants puisqu'ils peuvent faire perdre énormément d'argent mais aussi de la réputation à l'entreprise.

Nous allons donc prendre un exemple d'incident et déterminer son plan de continuité et de reprise d'activité informatique.

Entreprise : Tartempion, c'est une entreprise spécialisée dans le service informatique et l'architecture réseau. C'est une TPE composée de 5 salariés. Pour son activité principale, elle a besoin de prendre la main à distance sur les postes de ses clients via le logiciel Anydesk. Pour cela il lui faut un accès constant à internet. Elle effectue également des sauvegardes quotidiennes pour ses clients et les vérifie tous les jours.

Responsable : Théo Martin

Incident : une coupure de courant venant de l'extérieur (EDF)

Risques : ils sont nombreux : perte de données (sauvegarde), plus d'accès au serveur ni à internet etc…

Inventaire : l'entreprise possède 1 serveur, 5 PC avec double écrans, 5 téléphones IP, 1 box internet

Si une coupure de courant survenait, l'entreprise Tartempion se retrouverait sans ressource pour effectuer son travail. Pour une journée de travail sans électricité ni internet, la perte serait d'environ 1 500 euros.

Il faudrait donc trouver une ou plusieurs solutions pour éviter ce problème.

Le RTO (Recovery Time Objective = temps d'inactivité acceptable) ne doit pas dépasser 1h pour éviter de perdre trop de données non sauvegardées.

Premièrement il faudrait acquérir des onduleurs afin d'alimenter au moins les serveurs le temps de sauvegarder les données avant l'extinction progressive des services et l'attente de résolution d'incident.