IT Structure; cours 3

Plan :

-> Continuité d’Activité (PCA)

-> Risques impactant la PCA

…………….

### 1/ Introduction

#### Concepts clés

* **continuité informatique** : si y a un pb dans mon activité informatique, comment faire pour avoir accès à tout ce qui est matériel info (données sur serveurs, etc) ?
* **continuité des opérations** : comment faire en sorte qu’un service continue quand y a un pb? (genre dans les entreprises au self tu paies avec un badge, et si ton badge marche pas, quelles sont les actions la dame du self va entreprendre pour pas bloquer la caisse?)
* **gestion des incidents et des crises** : prendre par ex la décision de faire basculer d’un pc à un autre les infos en cas d’incident. Sauf que peut y avoir un pb ou autre. Du coup c’est quoi l’organisation mise en place qui va nous faire basculer ou pas (et comment) toutes nos infos en cas d’incident.

!!! attention : Le sens de l’acronyme PCA diffère selon le domaine où on en parle.

### 2/ Risque & menace

#### exemples & défintions

Lorsqu’il y a risque, y a tjr une menace avec une vulnérabilité.

*ex :*

*risque : malade -> plus pouvoir assister aux cours -> rater des exams;*

*menace : froid.*

qques **risques en entreprise** :

* grèves
* panne électrique
* inondation
* incendie
* panne logicielle
* panne matérielle
* séisme pandémie
* coupure informatique
* défaillance de prestataires
* …

pbs liés à l’erreur humaine : y en a en permanence.

menaces :

* wannacry mai 2017
* pannes électriques (mai 2017, juillet / novembre 2017)
* …

#### b) Comment traiter les risques?

ex : SI tombe en panne et on ne peut plus travailler

-> risque traité sur une **matrice d’options** :

* **accepter :** on accepte la menace et ses impacts pour l’entreprise
* **éviter :** ne pas lancer ou à arrêter une activité à cause des risques encourus
* **réduire la probabilité :** traiter le risque en amont, en réduisant sa probabilité d’occurrence
* **transférer :** déporter le risque sur un tiers (prise d’une assurance: ex cyber assurance pour les fuites de données)
* **limiter les impacts :** un peu le gilet pare balles.
* **PCA :** ensemble de dispositifs permettant de limiter les impacts lorsqu’un ou plusieurs scénarios de risques sont avérés

### 3/ Encore plus de définitions :

* **PCA** : englobe l’ensemble des actions, processus et organisations permettant la continuité **des activités critiques** de l’entreprise
* **PCI plan de continuité informatique** : (prévoir qqchose dans le cas où y a un pb, menace connue) on se focalise sur la disponibilité de tout ou une partie du système d’information
* en **cas d’incident / une panne** => On garantit la continuité de services au quotidien + la reprise pour les incidents compliqués
* **face à un sinistre majeur** => garantir la reprise d’activité sur sinistre majeur, ayant possiblement entraîné une perte de données dans un contexte fortement dégradé

⇒ relève du domaine du SI

*ex PCI:*

* *si t’as un SI qui recouvre toutes les activités, tu identifies des* ***activités critiques*** *et ce que tu cherches à secourir c’est ce qui va supporter ces activités critiques (applications, serveurs…)*

*(d’autres terminologies : PRI, PRA, PSI, DRP…)*

* **Cyber-résilience** (on connait pas la menace) = faire face à une menace non déterministe pouvant aussi affecter les dispositifs de secours

⇒ possiblement dans un contexte de perte de confiance dans le SI (postes, serveurs…, tu sais pas si ton serveur est compromis ou non) et des dispositifs de secours

* **cyber-résilience vs PCI :** le premier n’est pas prévisible alors que le second si

La continuité des activités informatiques est vitale pour celle des opérations.

* **PCO plan de continuité des opérations** : se focalise sur la poursuite des missions essentielles des métiers jugés vitaux face notamment à un sinistre majeur
* (ex : si y a plus d’électricité dans ma boulangerie, il faut un générateur de secours pour que je puisse continuer de fonctionner)/.

⇒ Relève du métier

### 4/ Deux notions : DIMA & PDMA

2 critères attendus dans l’expression de **besoin de continuité** :

* **DIMA (recovery TImes objective RTO)** = Durée d’interruption maximale admissible

⇒ délai de reprise

* **PDMA ( recovery Point objective RPO)** Perte de donnée maximale admissible

⇒ fraîcheur des informations

*//j’ai manqué le cours ici déso//*

### 5/ différentes composantes d’un PCA :

= organisation de crise

* **sites:** 
  + de repli
  + alternatifs
  + modes d’accès distants
* **informations télécoms :** pci
  + dispositifs de secours
  + procédures
  + organisation
  + ressources humaines
* **positions de travail :** ressources matérielles
  + poste de travail/applicatif
  + moyens de communication
  + équipements spécifiques
* **activités clefs**
  + mesures d’anticipation de contournement pour les activités vitales
* **organisation personnels**
  + personnel mobilisé
  + suppléance du personnel
  + acheminement du personnel
* f**ournisseurs prestataires**
  + engagement (contractuel) des prestataires vitaux

### 6/ Norme iso 22301

Une norme pour le pca : **iso 22301** = tout un tas de bonnes pratiques (parfaite continuité d’activité)

* **objectif** : piloter la continuité par les risques et entrer dans une démarche de progrès continu
* on prévoit de faire qqchose, on le fait, on vérifie qu’on l’a bien fait

### 7/ démarche d’élaboration d’un pca (c’est un processus continu)

**1 - cadrage** : analyse des scénarios risques & bilan d’impact sur l’activité (BIA)

* 1 / Recenser les menaces (facteurs naturels, environnementaux, techniques… Le + compliqué à gérer menaces internes)
* 2/ PSI indispo totale/partielle du SI
* 3/ PCO

**2 - Etat de l’Art/ benchmark & évaluation des scénarios**

|  |  |  |
| --- | --- | --- |
|  | **3 - conception** | **4 - mise en oeuvre** |
| **SI (PSI)** | **plan de secours IT** (organisation IT, infrastructures, procédures de reprise) | site & solutions de secours |
| **Métiers (PCO)** | **plan de secours métiers** (organisation, mesures préventives, procédures dégradées) | organisation |

**5** - **maintenance exercices & maj des plans**

**Les risques** = proba combinée avec les impacts

### 8/ identifier les menaces

ex de menace : la crue de Seine : bcp d’endroits touchés;

risques importants => bcp de mobilisation d’acteurs, de cibles de crises tout ça

Les menaces peuvent avoir des impacts multiples

* **image de la société** : ex victime d’une cyberattaque
* **interne** : ex caissière en peut plus de son travail car sa caisse fonctionne pas de matière optimale
* **financier :** pas assez de sous pour agir en mesure de variation boursière par ex
* l**égal** :
* **client** : le client cherche un plan B quand ça marche mal chez vous; mais quand ça remarche, il reviendra pas, il restera chez son plan B

### 9/ Grille d’impact

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| niveau d’impact | négligeable | limité | significatif | grave | extrêmement grave |
| impacts (perte financière, atteinte aux vies humaines, perte de productivité, retard…) |  |  |  |  |  |

### 10 / Le BIA

1. **processus critiques** :

* recenser les macros activités vitales à l’entreprise, qui sont les + sensibles (ce qui a un impact très fort sur l’entreprise)
* le délai d’interruption max admissible (DIMA)
* bilan d’impact “quantifiable” au sens de l’échelle d’impact

### 11 / Les étapes de ???

//là aussi j’ai manqué une partie jsp c’est les étapes de quoi du coup à voir avec les diapos

**Etape 2 :** **définir la stratégie pour le PSI (plan de secours informatique)**

* 2 stratégies : conception des solutions générales

1 / **définir les solutions de reprise possibles** => pour chaque couche du SI, étudier les solutions de reprise disponibles

2 / **construire les scénarios et sélectionner les pertinences** => construire les scénarios de reprise possibles et les sélectionner en fonction des besoins et des coûts

**Etape 3&4 : conception et mise en oeuvre**

conception et implémentation

**Etape 5 : Recette** (=tester tout ça)

* Pour améliorer la maturité des tests, il y a une approche progressive
* Test de gestion crise (ex)

**1/ tests unitaires** => on cherche à valider le bon fonctionnement des mécanismes & infrastructures

**2/ tests multi domaine** => valider le bon fonctionnement du secours d’un ensemble de composants techniques ou applicatifs

**3/ test de bascule applicative** => valide le bon fonctionnement des mécanismes de bascule & du fonctionnement en secours d’une à plusieurs applis

**4/ test de l’isolation du site** => fonctionnement de l’ensemble des mécanismes de secours

⇒ ce genre d’orga ça met du temps à être mis en place dans les entreprises

* faut définir des objectifs ambitieux et interpréter les tests correctement
* **un test réussi :**
* n’identifie pas d’incohérences ou de dysfonctionnements (ne correspond pas ou est très bien)
* le test peut être “challengeant” et faire face à des situations incertaines, mais n’est pas forcément raté

⇒ Trouver l’équilibre parfait entre actions à améliorer (dues aux défaillances) & confiance (en lien avec des tests réussis)

* **Simulation réaliste?**
* plus c’est réaliste & plus on a confiance dans notre PCA. Faut y aller doucement & pas prendre trop de risques à la fois.

**Etape 5 bis : maintenance & amélioration**

⇒ tests réguliers, maj des stratégies de secours, procédures techniques & procédures tout court

1/ Maj de la BIA

2/ adaptation de la stratégie

* **les composants d’un pci**
* secours des applications
* site de secours & d’hébergement
* secours des ressources
* secours des infrastructures
* référentiel documentaire
* collaborateurs impliqués
* l**es composantes de la continuité**

hébergement => réseaux et sécurité => stockage > …

(en gros c’est un peu l’ordre de ce qu’il faut couvrir en premier puis comment ça évolue de ce que j’ai compris)

// j’ai arrêté de suivre mais ça parlait des stratégies d’hébergement pour couvrir les risques

### 12/ stratégies de secours :

**1/ hébergement de secours**

⇒ selon la distance (de la plus petite couverture vers la plus grande couverture):

* + **sys répartis complexes** ( + près, niveau régional max 10 à 15km)
  + **sys répartis simples**
  + **réplication de données synchrone**
  + **réplication de données asynchrone** (marche très bien à de grandes distances > 200 km; niv national)
* Pour diminuer la perte de données il faut être + proche & diminuer la distance

mais + t’es proche + t’es exposé aux risques qui sont à 10 ou 20km.

⇒ faut trouver un juste milieu. Couvrir les risques mais aussi répondre aux demandes du métier

* **niveau de couverture par niveau (1 à 5)** : 1 couverture du sinistre local ⇒ sinistre de site majeur ⇒ sinistre majeur regional ⇒ snistre local de secours ⇒ sinistre majeur avec secours

Il y a plus de chances qu’il y ait un pb au niveau local que national (+ près = + risque)

**2/ secours des serveurs**

Pour faire de la disponibilité, faut avoir plusieurs serveurs un peu partout.

Adaptation du secours des serveurs aux délais de reprise souhaités selon **le temps** (du - lent au + ) :

**serveurs dédiés** : haute disponibilité (1 serveur s’arrête, l’autre continue) ⇒ activable ⇒ dormant ⇒ **serveurs mutualisés** : mutualisation interne || (même temps que) mutualisation fournisseur ⇒ **serveurs approvisionnés** : pré-contractualisation de l’approvisionnement “le jour où j’ai un pb j’achète un nouveau serveur” ⇒ approvisionnement en cas de sinistre

autres solutions :

* **solution de redondance** :
* **cluster système** : une machine reprend les services d’une autre, défaillante, en se réapproprient ses ressources
  + (ex : en cas de service normal, le client passe par le serveur normal pour accéder aux ressources de stockage; en cas de régime de secours, il passe par le serveur de secours)
* **cluster applicatif :** solution assurant la réplication des fonctions et/ou données pour assurer une redondance entre plusieurs machines
  + (ex : le client passe par la structure normale serveur 1 stockage 1, et en cas de problème il passe par la “copie”, serveur 2 et stockage 2)
* **solutions de virtualisation :** le secours est assuré en répliquant (via les mécanismes de baies SAN) la machine virtuelle (applications + données), qui peut être utilisée pour redémarrer en cas d’incident ( en cas de perte du serveur, on redémarre le sys dans exactement même état mais sur le serveur distant)

**2bis/ secours des serveurs (suite):**

* **réplication synchrone :** contraintes de distance mais en temps réel du coup facilite la synchronisation inter appli mais risque de corruption logique non couvert
* **réplication asynchrone :** perte de données limitées mais resynchronisation inter appli nécessaire
* **sauvegarde**; solution historique; en faire 1 tous les jours & s’assurer qu’elle soit bien effectuée
* Les contraintes les + exigeantes : **disponibilité distante synchrone**
* La contrainte la moins exigeante : **ressources approvisionnées;** on redémarre les serveurs avec les sauvegardes qu’on a faites. Mais on accepte de pas redémarrer tout de suite et perdre des données…

### 13/ les enjeux de disponibilité & continuité de + en + importants

Le si prend de la place partout (interdépendance des Si + transformation des métiers numériques qui sont de plus en plus présents sur le marché) y a une pression réglementaire continue (comme les banques, les assurances…)

### 14/ la manière dont on couvre…

* **les incidents locaux :** ça va à peu près c cool
* **sinistre de site :** un peu plus la merde, adoption ça va mais efficacité bof bof
* **sinistre régional :** encore plus la merde. Très peu d’adoption et presque pas d’efficacité

il faut **une adoption** et **une efficacité** des solutions proportionnelles aux incidents passés

nécessite une transformation de la production pour construire un PCI plus efficace

⇒ impératif pour la DSI & répondre aux enjeux

### 15 / les secours du Saas (cf cours de la semaine dernière)

* **3 tendances :**
* le secours est inclus (fournisseur a un site secondaire & sauvegarde) *ex : office 365*
* sauvegarde mais pas de plan de secours ( sauvegarde régulière, mais servent pas forcément pour le secours, un processus qu’est pas très clair)
* aucune prise en charge d’un moyen de plan de secours (pas de sauvegarde ni de secours… ex Winflotte)

**Travail en mode dégradé :**

1/ lister les activités vitales (BIA)

2/ déterminer les solutions de contournement possibles : formaliser de secours pour assurer la continuité métier durant la crise

3/ identifier les prérequis nécessaires aux solutions de contournement

4/ assurer la pérennité et le suivi du dispositif

### 15 / Gestion de crise

**Une crise** = situation soudaine, souvent brutale & inattendue aux conséquences potentiellement très graves pour l’entreprise et pour laquelle les mécanismes et les réactions sont inadaptées

⇒ gérer une crise efficacement

1/ détection (outils de supervision d’incident) de l’alerte (outils dédiés à la communication d’information interne)

2 / qualification

3/ déclenchement et traitement

4/ sortie de crise

Communication : élément clé de la gestion de crise