2018/2019

M2 Informatique Genie Logiciel Sûr (GLS)

TD GOUVERNANCE DE RISQUES

Produit par NDIAYE Babacar.

bndiaye0218@gmail.com

Professeur : Mr MARKUS Nicolas

nicowim.markus@gmail.com

Table des matières

Scénario 1 : arrêt des serveurs dû à leur surchauffe (intempéries climatiques)

1. Présentation du scénario

1.1. L'origine et les causes

Un aléa climatique est imprévisible et ne peut être mesuré avec exactitude, même si les précautions nécessaires sont prises dans les salle serveurs pour lutter contre la surchauffe, une forte canicule peut entraîner la chute de certains serveurs.

1.2. Les conséquences

Les conséquences dans le cas d'un système avec redondance bien que minime seront quand même présente :

- Services indisponibles pendant le temps de la bascule serveurs, entre 5 à 30mn soit une valeur de 6000k€/heure pour une structure de e-commerce et une valeur de 1k€/min pour un service public comme une mairie (perte estimée en fonction de temps de travail pour les agents publics)
- Perte de travail, la mémoire vive du serveur ayant des données avant la chute seront perdu.

1.3. Les variantes possibles

Ce risque a la possibilité de se réaliser sous diverses formes en fonction :

- Interruption momentané du serveur
- Interruption d'un serveur et le redondant tjrs disponible
- Interruption de tous les serveurs y compris celui redondé (cette variante a des conséquences très grave mais a peu de chance de se produire)

2. Détail du scénario

2.1. Les modes de reprise

- Reprise par balance sur le serveur redondé, ce mode la sera le plus privilégié pour un système redondant
- Reprise par redémarrage du serveur, ce mode plus risqué peut provoquer la rechute du serveur et arrêt des services(déconseillé)

2.2. Planning de reprise

Après la détection de ce risque les étapes suivantes seront à respecter pour s'assurer de la bonne reprise et la stabilité du système :

- Lancer un communiquer d'information du personnel et de tous service ou entreprise dépendant des services proposés par le serveur
- Lancer le processus de bascule des services sur le serveur redondant

- Dépêcher un agent en salle serveur pour débrancher le serveur atteint de surchauffe et attendre son refroidissement
- Eteindre tous les serveurs susceptibles de surchauffer si ceux-ci ont un serveur associé dans une autre salle
- Après refroidissement du serveur lancer la récupération des données de la mémoire vive
- Vérifier l'état de la mémoire et relancer le serveur
- Assurer une surveillance du serveur pendant un temps minimum de 24h

2.3.Réaction après résolution de l'incident

- Estimée les pertes financières
- Réétudier la viabilité de la position géographique de la salle serveur
- Et faire un bilan de l'expérience acquise

3. Position dans la matrice de risque

Dans la matrice des risques (en annexe) cette incident a un risque **3(risque à suivre)** avec des conséquences majeures et une probabilité moyenne de se réaliser.

Scénario 2: cryptage des fichiers de l'entreprise dû à une attaque du type ransomeware wanacrypt

1. Présentation du scénario

1.1. *L'origine et les causes*

Les attaques informatiques sont prévisibles, mais ne peut être totalement évité, notamment celle qui concerne directement les utilisateurs qui n'ont pas forcement connaissance de leur existence. Un email de reçus, puis un click par inadvertance ou curiosité, et voilà un incident risqué pour toute l'entreprise.

1.2. *Les conséquences*

Cas d'une ransomeware wanacrypt :

- Impossibilité de travaillé pour tous les agent atteint
- Perte des ressources (dossier et fichier)
- Perte financière paiement de rançon pour obtenir clé de décryptage entre 2k€ et 5k€ par agent, pris individuellement cette perte financière parait minime mais si plusieurs agents ont été victime de l'attaque ce montant parais énorme.

1.3. *Les variantes possibles*

Les variantes de ce risque sont :

- Atteinte de tout le système via cette attaque (conséquence financière catastrophique)
- Atteinte d'une partie du parc informatique
- Atteinte d'un seul agent

2. Détail du scénario

2.1. Mode de reprise

- reprise des fichier grâce à l'aide des partenaires disposant peut-être d'une solution

- reprise en payant la rançon

- reprise par achat d'anti-virus ayant un protocole de décryptage

2.2. *Planning de reprise*

- Informer les utilisateurs du problème de sécurité dès la détection

- Augmenter la surveillance des serveurs et de la partie du parc informatique non atteinte par la menace

- Vérifier auprès des partenaires de l'entreprise s'il détienne une solution pour le décryptage des données

- Négocier avec les attaquants le montant des clés

- Payer la rançon et augmenter la sécurité du réseau

2.3. *Réaction après résolution de l'incident*

- Renforcer la sécurité du système (en fessant le trie d'email ou la non apparition des lien)

- Faire une formation au agents de l'entreprise pour la prise en compte du risque

3. Position dans la matrice de risque

Dans la matrice des risques (en annexe) cette incident a un risque **4(risque sévère)** c'est-à-dire qu'il est peu probable par contre il a des conséquences catastrophiques.

ANNEXE

MATRICE DES RISQUES

	Négligeable	Mineur	Moderé	Majeur	Critique	Catastrophique
Très probable	2	3	4	4	4	4
Probable	2	2	3	4	4	4
moyennementProbable	1	2	3	3	4	4
peu probable	1	2	2	3	3	4
faiblement probable	1	1	2	2	3	4
très faiblement probable	1	1	1	1	2	4