

2024

DIRECTION DU SYSTEME D'INFORMATION

Destinataire :
Services Informatiques



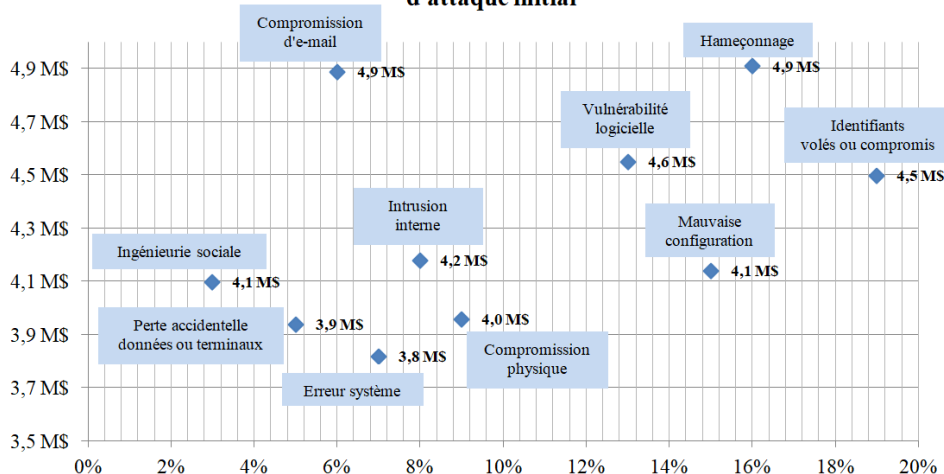
Peu importe la cause (cybercriminalité, erreur humaine, défaillance de logiciel et/ou matérielle, catastrophe naturelle, ...) ou la durée de la panne (de quelques heures à quelques semaines) : un sinistre informatique a toujours de lourdes conséquences économiques, difficilement mesurables.

Les évolutions récentes du système d'information de THOLDI ont mis en évidence un certain nombre de failles ou d'insuffisances en termes d'infrastructure et de solutions applicatives.

La DSI s'appuie notamment sur plusieurs études :

- D'après l'étude *Global Data Protection Index de 2021*, « le coût moyen de la perte de données en 2021 était de 930 247 € et le coût moyen de l'interruption de service non planifiée était de 500 558 €. »
- Selon un rapport de l'*Uptime Institute*, « les pannes entraînant des pertes de plus de 100 000 \$ sont passées de 40% en 2020 à 47% en 2021. L'institut rapporte également qu'au cours des trois dernières années, une entreprise sur cinq a subi une panne importante, engendrant des coûts très élevés, des atteintes à la réputation ou même des violations de la conformité. »
- Selon une autre étude de *Nexthink* en avril 2020, « les collaborateurs perdent deux semaines de travail par an suite à des dysfonctionnements informatiques. »
- Selon *IBM*, « le coût moyen d'une violation de données en 2023 était de 4,45 millions \$, soit une augmentation de 15 % en 3 ans. »

Coût moyen et fréquence des violations de données par vecteur d'attaque initial



[PROJET HA]

Projet High Availability

À la suite d'un **audit**, la direction des systèmes d'information (DSI) doit mettre en œuvre tous les moyens qui permettront **d'accroître la disponibilité** et la **cohérence du système d'information**.

Fort de cette analyse, la DSI a élaboré un **contrat de service** qui définit :

- Les services attendus et leur niveau requis (SLA¹).
- Un niveau de qualité.
- Les responsabilités des services Analyse & Développement et Infrastructure & Système.
- Les modalités de contrôle et les indicateurs de mesure de la performance.
- Les solutions palliatives en cas de défaillances.

Ce contrat de service a permis, au niveau opérationnel, de mettre en évidence plusieurs projets, notamment les suivants :

PROJET « APPLI MOB »

Au niveau du développement applicatif, la mise en place de processus adaptés permet de **réduire les erreurs**, et **d'augmenter la cohérence du système d'information**. Dans cette optique deux missions vous seront proposées afin de garantir la sécurisation d'une base de données avant de développer une application mobile.

- Mission n°1 : Préparation et sécurisation de la base de données
- Mission n°2 : Développement de l'application mobile utilisatrice d'un service web

PROJET « HIGH AVAILABILITY » (HA)

Au niveau de l'infrastructure Réseau & Système, le **Plan de Reprise d'Activité (PRA)** doit être associé à un **Plan de Continuité d'Activité (PCA)**.

Le PCA vise plus particulièrement la haute disponibilité de l'infrastructure et des services selon les taux de disponibilité choisis (voir annexe 4).

Plusieurs missions doivent être menées :

- Mission n°1 : Haute disponibilité de l'infrastructure Ethernet (STP)
- Mission n°2 : Haute disponibilité des services de fichiers (NAS)
- Mission n°3 : Haute disponibilité du service WEB
- Mission n°4 : Supervision des services et de l'infrastructure.

¹ Le Service Level Agreement (SLA) est un contrat de service qui définit le périmètre de la prestation et la qualité de service requise entre un prestataire et un client.

PROJET « APPLIMOB »

Solutions Logicielles et Applications Métier

Application de demande de réservation d'emplacements dans la zone de stockage mise à disposition de la société Tholdi

MISSION N°1 : PRÉPARATION ET SÉCURISATION DE LA BASE DE DONNÉES

- Analyse du cahier des charges d'un service à produire
- Étude des exigences liées à la qualité attendue d'un service
- Rédaction des spécifications techniques de la solution retenue (adaptation d'une solution existante ou réalisation d'une nouvelle solution)
- Évaluation des risques liés à l'utilisation d'un service
- Détermination des tests nécessaires à la validation d'un service
- Test d'intégration et d'acceptation d'un service
- Définition des éléments nécessaires à la continuité d'un service
- Accompagnement de la mise en place d'un nouveau service
- Participation à un projet
- Évaluation des indicateurs de suivi d'un projet et justification des écarts
- Gestion des ressources
- Évaluation et maintien de la qualité d'un service
- Suivi et résolution d'incidents
- Réponse à une interruption de service
- Identification, qualification et évaluation d'un problème
- Planification des sauvegardes et gestion des restaurations
- Conception ou adaptation d'une base de données
- Rédaction d'une documentation technique
- Rédaction d'une documentation d'utilisation
- Analyse et correction d'un dysfonctionnement, d'un problème de qualité de service ou de sécurité
- Adaptation d'une solution applicative aux évolutions de ses composants
- Mise à jour d'une documentation technique
- Exploitation des référentiels, normes et standards adoptés par le prestataire informatique
- Veille technologique
- Repérage des compléments de formation ou d'auto-formation utiles à l'acquisition de nouvelles compétences

MISSION N°2 : DÉVELOPPEMENT DE L'APPLICATION MOBILE UTILISATRICE D'UN « WEB SERVICE »

- Analyse du cahier des charges d'un service à produire
- Étude des exigences liées à la qualité attendue d'un service
- Rédaction des spécifications techniques de la solution retenue (adaptation d'une solution existante ou réalisation d'une nouvelle solution)
- Évaluation des risques liés à l'utilisation d'un service
- Détermination des tests nécessaires à la validation d'un service
- Test d'intégration et d'acceptation d'un service
- Définition des éléments nécessaires à la continuité d'un service
- Accompagnement de la mise en place d'un nouveau service
- Déploiement d'un service
- Participation à un projet
- Évaluation des indicateurs de suivi d'un projet et justification des écarts
- Gestion des ressources
- Accompagnement des utilisateurs dans la prise en main d'un service
- Évaluation et maintien de la qualité d'un service
- Suivi et résolution d'incidents
- Réponse à une interruption de service
- Identification, qualification et évaluation d'un problème
- Maquettage et prototypage d'une solution d'infrastructure
- Proposition d'une solution applicative
- Conception ou adaptation de l'interface utilisateur d'une solution applicative
- Définition des caractéristiques d'une solution applicative
- Prototypage de composants logiciels
- Gestion d'environnements de développement et de test
- Développement, utilisation ou adaptation de composants logiciels
- Réalisation des tests nécessaires à la validation d'éléments adaptés ou développés
- Rédaction d'une documentation technique
- Rédaction d'une documentation d'utilisation
- Analyse et correction d'un dysfonctionnement, d'un problème de qualité de service ou de sécurité
- Adaptation d'une solution applicative aux évolutions de ses composants
- Réalisation des tests nécessaires à la mise en production d'éléments mis à jour
- Mise à jour d'une documentation technique
- Exploitation des référentiels, normes et standards adoptés par le prestataire informatique
- Veille technologique
- Repérage des compléments de formation ou d'auto-formation utiles à l'acquisition de nouvelles compétences
- Étude d'une technologie, d'un composant, d'un outil ou d'une méthode

PROJET « HA »

Solutions d'Infrastructures, Systèmes et Réseaux **High Availability**

MISSION N°1 : HAUTE DISPONIBILITÉ DE L'INFRASTRUCTURE ETHERNET (STP)

- Analyse du cahier des charges d'un service à produire
- Étude de l'impact de l'intégration d'un service
- Rédaction des spécifications techniques de la solution retenue
- Détermination des tests nécessaires à la validation
- Test d'intégration et d'acceptation d'un service
- Participation à un projet
- Évaluation des indicateurs de suivi d'un projet et justification des écarts
- Gestion des ressources
- Réponse à une interruption de service
- Proposition d'une solution d'infrastructure
- Installation et configuration d'éléments d'infrastructure
- Mise à jour de la documentation technique
- Administration sur site ou à distance des éléments d'un réseau, de serveurs, de services et d'équipements
- Étude d'une technologie, d'un composant, d'un outil

MISSION N°2 : HAUTE DISPONIBILITÉ DES SERVICES DE FICHIERS (NAS)

- Analyse du cahier des charges d'un service à produire
- Étude de l'impact de l'intégration d'un service
- Étude des exigences liées à la qualité attendue d'un service
- Rédaction des spécifications techniques de la solution retenue
- Détermination des tests nécessaires à la validation
- Définition des niveaux d'habilitation
- Test d'intégration et d'acceptation d'un service
- Définition des éléments nécessaires à la continuité
- Déploiement d'un service
- Participation à un projet
- Évaluation des indicateurs de suivi d'un projet et justification des écarts
- Évaluation et maintien de la qualité d'un service
- Proposition d'amélioration d'un service
- Proposition d'une solution d'infrastructure
- Prise en compte du niveau de sécurité nécessaire à une infrastructure
- Installation et configuration d'éléments d'infrastructure
- Mise à jour de la documentation technique
- Planification des sauvegardes et gestion des restaurations
- Automatisation des tâches d'administration
- Étude de propositions de contrat de service (client, fournisseur)
- Exploitation des référentiels, normes et standard
- Veille technologique
- Étude d'une technologie, d'un composant, d'un outil

MISSION N°3 : HAUTE DISPONIBILITÉ DU SERVICE WEB

- Analyse du cahier des charges d'un service à produire
- Étude de l'impact de l'intégration d'un service
- Étude des exigences liées à la qualité attendue d'un service
- Rédaction des spécifications techniques de la solution retenue (adaptation d'une solution existante ou réalisation d'une nouvelle solution)
- Évaluation des risques liés à l'utilisation d'un service
- Détermination des tests nécessaires à la validation d'un service
- Test d'intégration et d'acceptation d'un service
- Définition des éléments nécessaires à la continuité
- Participation à un projet
- Évaluation des indicateurs de suivi d'un projet et justification des écarts
- Évaluation et maintien de la qualité d'un service
- Réponse à une interruption de service
- Proposition d'amélioration d'un service
- Proposition d'une solution d'infrastructure
- Installation et configuration d'éléments d'infrastructure
- Mise à jour de la documentation technique d'une solution d'infrastructure
- Étude de propositions de contrat de service (client, fournisseur)
- Veille technologique
- Étude d'une technologie, d'un composant, d'un outil

MISSION N°4 : SUPERVISION DES SERVICES ET DE L'INFRASTRUCTURE.

- Analyse du cahier des charges d'un service à produire
- Étude de l'impact de l'intégration d'un service
- Étude des exigences liées à la qualité attendue d'un service
- Test d'intégration et d'acceptation d'un service
- Définition des éléments nécessaires à la continuité
- Évaluation et maintien de la qualité d'un service
- Identification, qualification et évaluation d'un problème
- Gestion des indicateurs et des fichiers d'activité
- Recueil d'informations sur une configuration et ses éléments
- Suivi d'une configuration et de ses éléments
- Étude de propositions de contrat de service (client, fournisseur)
- Exploitation des référentiels, normes et standards adoptés par le prestataire informatique
- Veille technologique
- Repérage des compléments de formation ou d'auto-formation utiles à l'acquisition de nouvelles compétences
- Étude d'une technologie, d'un composant, d'un outil

GESTION DE PROJET

RESPONSABILITÉS

Les groupes de projet sont constitués en complémentarité de compétences : une équipe de « développement » et une équipe « réseau & système ».

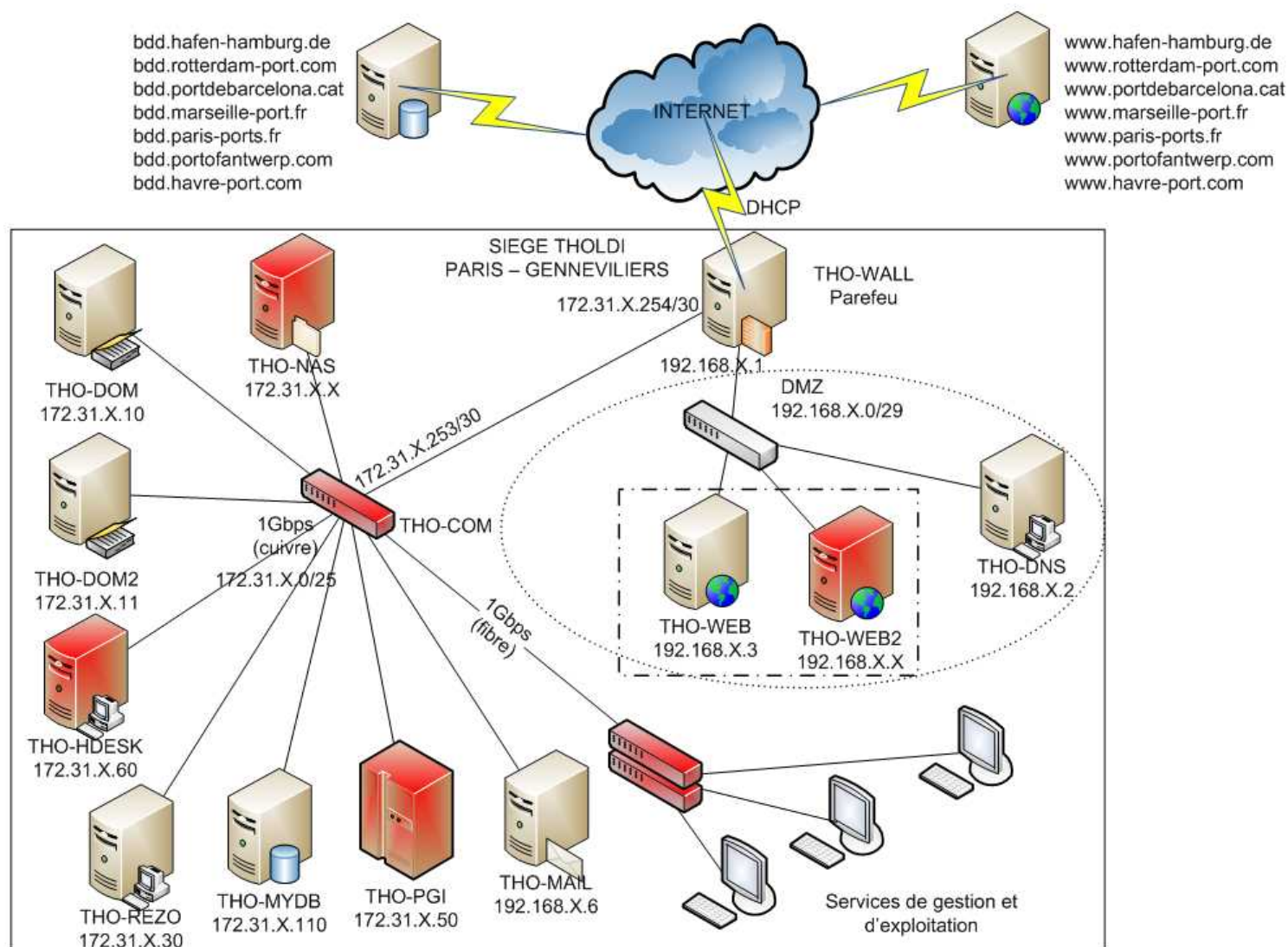
Chaque membre d'un groupe partage la responsabilité du projet et peut être l'interlocuteur de la DSI. La coordination des tâches à réaliser, le respect des échéances, la qualité des livrables, et la finalisation de la documentation sont autant de points d'évaluation.

Les cahiers des charges fonctionnels sont fournis en annexes, ainsi que des documents de travail.


ÉCHÉANCE DU PROJET FIXÉE AU 05/04/2024

Jalons SLAM	Dates	Jalons SISR
<ul style="list-style-type: none"> - Analyse du cahier des charges - Mise à jour BDD (structure et jeu d'essai) - Rétro-conception - Définition des besoins pour l'optimisation de la base de données 	01/03/2024	<ul style="list-style-type: none"> - Analyse du cahier des charges - Élaboration du contrat de service (M4)
<ul style="list-style-type: none"> - Application mobile AppliDemande (utilisation du Web Service) - IHM Réservation - Insertion et Consultation des demandes de réservation 	08/03/2024	<ul style="list-style-type: none"> - Installation du serveur THO-NAS (M2) - Mise en œuvre d'un RAID sur THO-NAS - Installation de NAGIOS sur THO-HDESK - Configuration de NAGIOS pour la supervision passive des serveurs - Configuration de HeartBeat sur THO-WEB
<ul style="list-style-type: none"> - Modification et Suppression des demandes de réservation - Procédures stockées / Fonctions stockées 	15/03/2024	<ul style="list-style-type: none"> - STP opérationnel sur les commutateurs (M1) - Installation et configuration du service FTP sur THO-NAS
	22/03/2024	<ul style="list-style-type: none"> - Scripting de sauvegarde des bases de données Mysql sur THO-NAS - Configuration de NAGIOS pour la supervision passive des services
<ul style="list-style-type: none"> - Triggers - Validation d'une demande de réservation (passer de l'état « demande » à « en cours ») 	29/03/2024	<ul style="list-style-type: none"> - Scripting de sauvegarde des bases de données Postgresql sur THO-NAS - Configuration de DRBD sur THO-WEB - Configuration de NAGIOS pour la supervision active des serveurs (charge processeur, espace disques) et switches
	05/04/2024	<ul style="list-style-type: none"> - Scripting de sauvegarde des journaux sur THO-NAS - Haute disponibilité du service web (DMZ) - Rapport d'activité de la supervision

Annexe 1: Infrastructure THOLDI – Site de Paris Gennevilliers



Annexe 2: « AWS raconte l'origine de sa dernière grande panne informatique »

 <p>https://www.zdnet.fr Par Liam Tung 13 Décembre 2021</p>	<p>Technologie : <i>Après s'être excusé pour une longue panne survenue sur sa plateforme, AWS l'a justifié par un problème de traduction d'adresses entre son réseau principal et son réseau interne.</i></p>
---	--

Amazon Web Services (AWS) tombe rarement en panne de manière inattendue, mais lorsque cela survient, le géant américain du cloud computing fait généralement preuve de transparence. La preuve après l'une des dernières pannes majeures d'AWS survenue mardi dernier. Celle-ci a duré cinq heures et a affecté les clients utilisant certaines interfaces d'application outre-Atlantique. Dans un cloud public de l'envergure d'AWS, une panne de cinq heures est un incident majeur.

Selon l'explication d'AWS sur ce qui s'est passé, la source de la panne était un problème dans son réseau interne qui héberge des « services fondamentaux » comme la surveillance des applications/services, le service de nom de domaine (DNS) interne d'AWS, l'autorisation et des parties du plan de contrôle du réseau Elastic Cloud 2 (EC2). Le DNS était important dans ce cas, car il s'agit du système utilisé pour traduire les noms de domaine lisibles par l'homme en adresses numériques internet (IP).

Le réseau interne d'AWS est à la base de certaines parties de son réseau principal, auquel la plupart des clients se connectent pour fournir leurs services de contenu. Normalement, lorsque le réseau principal s'étend pour répondre à une augmentation de la demande de ressources, le réseau interne devrait s'étendre proportionnellement via des dispositifs de mise en réseau qui gèrent la traduction d'adresses réseau (NAT) entre les deux réseaux. Ce mardi, la mise à l'échelle inter-réseaux ne s'est toutefois pas déroulée sans heurts, les dispositifs NAT d'AWS sur le réseau interne étant « débordés » et bloquant les messages de traduction entre les réseaux, ce qui a eu de graves répercussions sur plusieurs services clients qui, techniquement, n'ont pas été directement touchés.

« Une activité automatisée visant à mettre à l'échelle la capacité de l'un des services AWS hébergés dans le réseau AWS principal a déclenché un comportement inattendu de la part d'un grand nombre de clients à l'intérieur du réseau interne », indique AWS dans un post d'entreprise. « Cela a entraîné une forte augmentation de l'activité de connexion qui a submergé les dispositifs de mise en réseau entre le réseau interne et le réseau AWS principal, entraînant

des retards pour la communication entre ces réseaux. » Ces retards ont engendré de la latence et des erreurs pour les services fondamentaux parlant entre les réseaux, déclenchant encore plus de tentatives de connexion ratées qui ont finalement conduit à « des problèmes persistants de congestion et de performance » sur les dispositifs du réseau interne.

La connexion entre les deux réseaux étant bloquée, l'équipe d'exploitation interne d'AWS a rapidement perdu la visibilité de ses services de surveillance en temps réel et a dû se fier aux journaux d'événements passés pour déterminer la cause de la congestion. Après avoir identifié un pic d'erreurs DNS internes, les équipes ont détourné le trafic DNS interne des chemins bloqués. Ce travail a été achevé deux heures après la panne initiale. Cela a permis d'atténuer l'impact sur les services destinés aux clients, mais n'a pas permis de réparer complètement les services AWS affectés ni de débloquer la congestion des dispositifs NAT. En outre, l'équipe d'exploitation interne d'AWS ne disposait toujours pas de données de surveillance en temps réel, ce qui a ralenti la reprise et la restauration.

Outre le manque de visibilité en temps réel, les systèmes de déploiement internes d'AWS étaient entravés, ce qui ralentissait à nouveau les mesures correctives. La troisième cause majeure de cette réponse non optimale était la crainte qu'une correction des communications entre le réseau interne et le réseau principal ne perturbe d'autres services AWS orientés client qui n'étaient pas affectés. « Étant donné que de nombreux services AWS sur le réseau principal AWS et les applications des clients AWS fonctionnaient encore normalement, nous avons voulu être extrêmement prudents lors des modifications afin d'éviter d'avoir un impact sur les charges de travail en cours », ont fait savoir les équipes d'AWS.

[...]

Annexe 3: Calculer le coût d'une panne informatique

Il est important de se rendre compte des coûts possibles à déboursier pour son entreprise en cas de panne.

■ Calcul du coût de l'indisponibilité

Calculer le coût de l'indisponibilité permet entre autres d'adapter votre stratégie en fonction des coûts supportables ou non pour votre entreprise.

Coût de l'indisponibilité = perte de CA + perte de productivité + coût de la restauration + frais indirects + impact sur l'image de marque

✓ Calcul de la perte de CA

Une panne informatique peut durer plusieurs heures voire plusieurs jours. Il est donc important de calculer son impact sur le chiffre d'affaires global de l'entreprise.

Dans un premier temps, il est nécessaire de calculer le chiffre d'affaires horaire : CA hebdomadaire / 35h

Suite à ça, vous pourrez calculer la perte de CA avec cette formule :

Coût de la perte de chiffre d'affaires = CA horaire x temps d'interruption x pourcentage de disponibilité

✓ Calcul de la perte de productivité

La panne de l'infrastructure informatique impacte forcément sur la productivité de l'entreprise. En effet, si les collaborateurs n'ont pas accès à leurs données numériques, essentielles pour travailler, la productivité sera impactée. Selon le poste de l'employé certains pourront peut-être continuer de travailler.

Coût de la perte de productivité = (Salaire horaire du salarié n°1 x % de productivité) + (Salaire horaire du salarié n°2 x % de productivité) + etc.

■ Anticiper et réduire le coût des pannes informatiques

Afin d'éviter de déboursier des sommes astronomiques, nous vous conseillons d'anticiper les éventuels problèmes en mettant différentes mesures :

✓ Préparer un PCA :

Le Plan de Continuité d'Activité (**PCA**) a pour objectif de garantir le bon fonctionnement du système d'information en cas de panne ou d'incident.

Les solutions communes sont la redondance de ressources de type « failover » (une ressource active, une autre en attente) ou « load balancing » (plusieurs ressources actives en même temps).

✓ Préparer un PRA :

Le Plan de Reprise d'Activité (**PRA**) regroupe des mesures permettant de rétablir et de reprendre rapidement l'activité de l'entreprise. Il est important de noter que le PRA est un outil qui doit être mis à jour régulièrement en fonction du développement de l'entreprise.

Afin de réduire les risques de pertes de données lors d'une panne informatique, il est important de choisir une solution de sauvegarde efficace et adaptée. Plusieurs types de sauvegardes sont possibles (sauvegarde locale, externalisée, hybride).

✓ Former ses équipes :

Selon l'étude Coast of Data Breach Study 2020, 21% de la violation de la confidentialité des données est provoquée par une erreur humaine.

Il est donc nécessaire de sensibiliser et de former ses collaborateurs à la cybersécurité.



Annexe 4: Haute disponibilité ?

■ La disponibilité se mesure souvent en pourcentage :

Disponibilité en %	Indisponibilité par année	Indisponibilité par semaine	Indisponibilité par jour
90 % (« un neuf »)	36,5 jours	16,8 heures	2,4 heures
99 % (« deux neuf »)	3,65 jours	1,68 heures	14,4 minutes
99,9 % (« trois neuf »)	8,76 heures	10,1 minutes	1,44 minute
99,99 % (« quatre neuf »)	52,56 minutes	1,01 minute	8,64 secondes
99,999 % (« cinq neuf »)	5,26 minutes	6,05 secondes	0,864 seconde
99,9999 % (« six neuf »)	31,5 secondes	0,605 secondes	86,4 millisecondes

■ Dépendance vis-à-vis de l'infrastructure

Pour chaque niveau de l'architecture, pour chaque composant, chaque liaison entre composants, il faut établir :

- Comment détecter une panne ? Exemples : Tests de vie TCP Health Check implémenté par un boîtier Alteon, programme de test invoqué périodiquement (« nagios », « heartbeat »), interface de type « diagnostic » sur les composants...
- Comment le composant est-il sécurisé, redondé, secouru... Exemples : serveur de secours, cluster système, clustering Websphere, stockage RAID, sauvegardes, double attachement SAN, mode dégradé, matériel non utilisé libre (spare) prêt à être réinstallé..
- Comment désire-t-on enclencher la bascule en mode secours / dégradé. Manuellement après analyse ? Automatiquement ?
- Comment s'assurer que le système de secours reparte sur un état stable et connu. Exemples : on repart d'une copie de la base et on réapplique les archives logs, relance des batchs depuis un état connu, commit à 2 phases pour les transactions mettant à jour plusieurs gisements de données...
- Comment l'application redémarre sur le mécanisme de secours. Exemples : redémarrage de l'application, redémarrage des batchs interrompus, activation d'un mode dégradé, reprise de l'adresse IP du serveur défaillant par le serveur de secours...
- Comment reprendre éventuellement les transactions ou sessions en cours. Exemples : persistance de session sur le serveur applicatif, mécanisme pour assurer une réponse à un client pour une transaction qui s'est bien effectuée avant défaillance mais pour laquelle le client n'a pas eu de réponse...
- Comment revenir à la situation nominale. Exemples :
 - si un mode dégradé permet en cas de défaillance d'une base de données de stocker des transactions en attente dans un fichier, comment les transactions sont-elles ré-appliquées quand la base de données redevient active.
 - si un composant défaillant a été désactivé, comment s'effectue sa réintroduction en service actif (nécessité par exemple de resynchroniser des données, de retester le composant...)

■ Dépendance vis-à-vis des autres applications

- Pour une application qui sollicite d'autres applications avec des middlewares en mode synchrone (service webs en http, Tuxedo, Corba, EJB) le taux de disponibilité de l'application sera fortement lié à la disponibilité des applications dont elle dépend. La sensibilité des applications dont on dépend doit donc être équivalente ou supérieure à la sensibilité de l'application elle-même.

http://fr.wikipedia.org/wiki/Haute_disponibilit%C3%A9

<http://www.haute-disponibilite.net/2009/09/28/mesure-de-la-disponibilite-d-un-service>