Cyberattaque et sauvegarde des données

Quels backups mettre en place dans votre organisation ?

Union des Villes et Communes de Wallonie asbl

Wallonie

Webinaire – 19 octobre 2022

Nos invités

Olivier COLLET
Chief Information Security Officer
iMio

Andy SCHREURS
Directeur
HelpiT

Benoit JOSEPH
Directeur
Service Informatique
Ville de Liège

Menu de la séance

01 Sauvegarde des données : quelles sont les différentes options technologiques et méthodes de backup ?

02 Retour d'expérience : quels systèmes de sauvegarde ont été mis en place à la Ville de Liège ?

03 Centrale d'achats « cybersécurité » : quel accompagnement d'iMio aux pouvoirs locaux wallons ?

01 02 03

Sauvegarde des données : quelles sont les différentes options technologiques et méthodes de backup ?

Andy Schreurs

HelpiT

Sauvegarde des données

Andy Schreurs

Ceo & Founder de HelpIT

Depuis plus de 15 ans dans la gestion informatique

HelpiT

NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Sauvegarde des données

1) Quels sont les différents types de backups et leurs avantages/inconvénients ?

2) Comment doit être effectuée la sauvegarde ?

3) Quand et à quelle fréquence effectuer vos sauvegardes ?

4) Renforcer son système, c'est aussi anticiper la restauration des données.
   Quel système de restauration des données privilégier ?

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

1. Quels sont les différents types de backups et leurs avantages/inconvénients ?

La sauvegarde complète copie l'intégralité de vos données à un instant T.

Avantage :

- Sauvegarde la plus simple à réaliser et à restaurer

Inconvénient :

- Nécessite plus de temps pour s'effectuer et utilise un plus gros espace de stockage

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

La sauvegarde différentielle exécute une 1re sauvegarde complète des données. Ensuite, seuls les fichiers modifiés et ajoutés depuis la dernière sauvegarde complète sont sauvegardés.

Avantages :

- Restauration des données faite plus rapidement
- Pas de risque d'erreurs car vous n'utiliserez que la dernière sauvegarde complète

Inconvénient :

- Temps de restauration plus court mais nécessite un plus grand espace de stockage que l'incrémentale

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

La sauvegarde incrémentale, même principe que la sauvegarde différentielle, une 1re sauvegarde complète, mais lors de la prochaine sauvegarde, seules les modifications apportées depuis la dernière sauvegarde incrémentale effectuée seront sauvegardées.

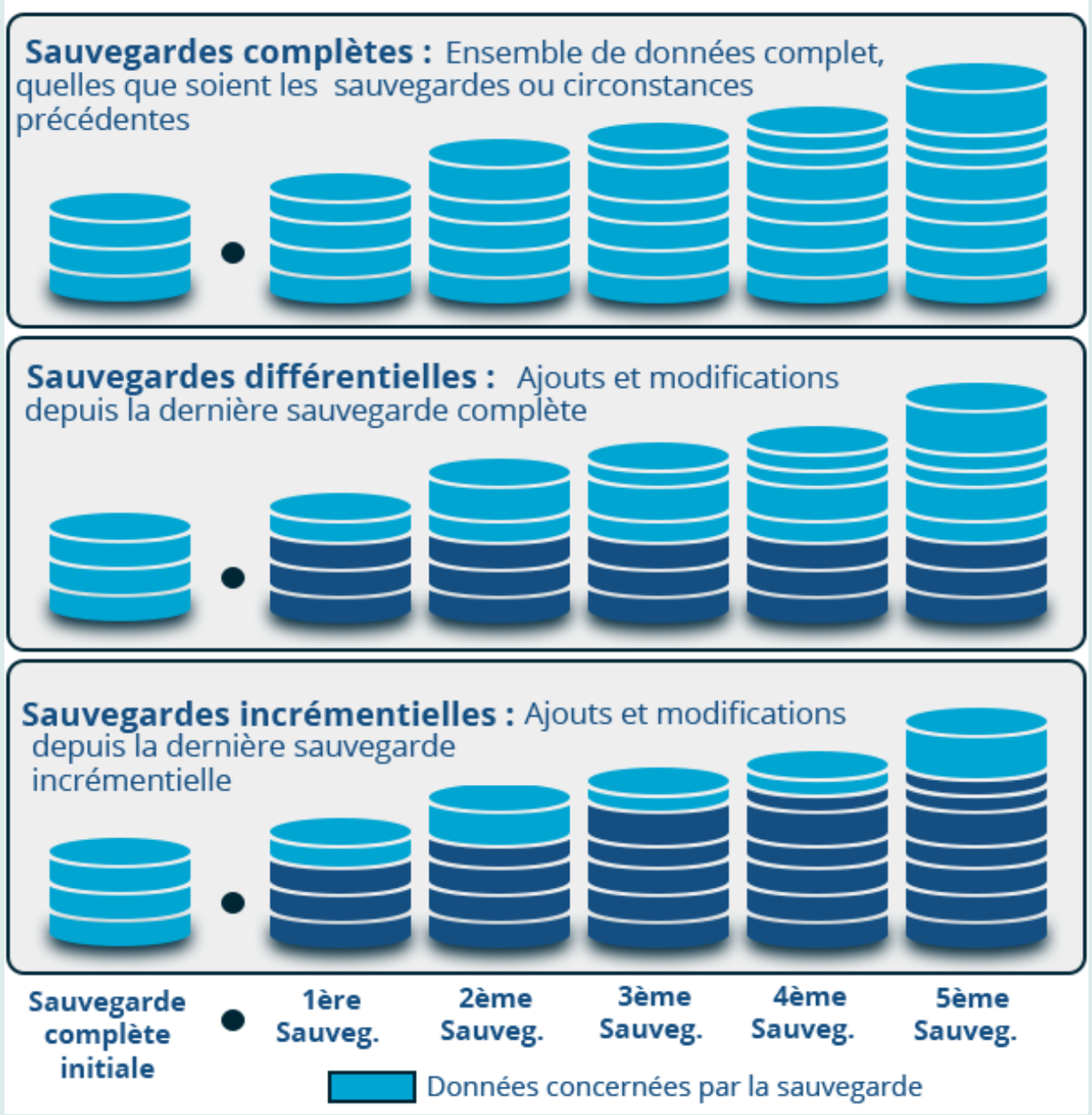
Avantages :

- Moins d'espace de stockage nécessaire
- Moins de bande passante
- Sauvegarde plus rapide qu'une sauvegarde complète

Inconvénient :

- Temps de restauration plus long car toutes les sauvegardes doivent être regroupées pour restaurer l'entièreté de vos données

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE



HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Cependant, ce choix est de nos jours simplifié et automatisé :

- Des solutions de sauvegarde (logiciels) utilisent un mix des technologies « complète », « incrémentale » et « différentielle », de manière automatisée pour optimiser le temps de sauvegarde ainsi que la gestion et restauration.

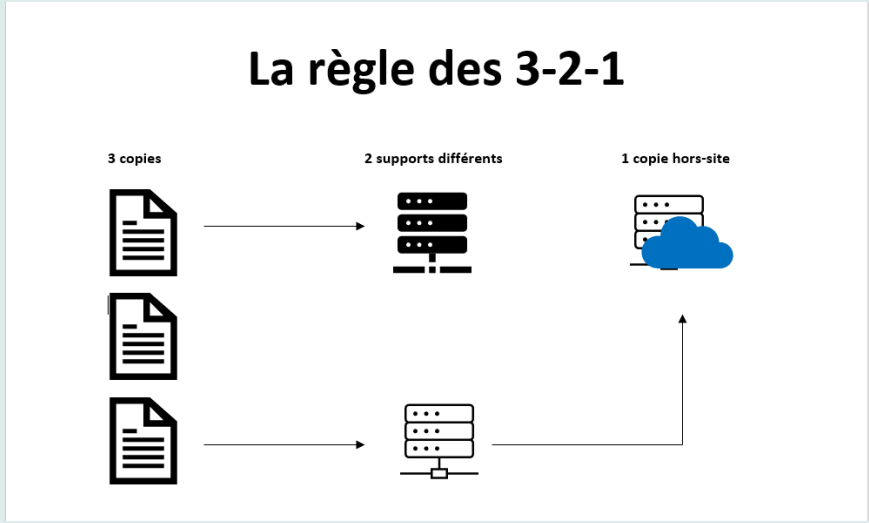
- Il peut y avoir une notion de Versionning : conserver plusieurs versions d'un même fichier en fonction de la fréquence de sauvegarde et du quota, du nombre de jours, mois, année choisie.

Si vous possédez des machines virtuelles, il existe d'autres techniques de sauvegarde et snapshot.

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

2. Comment doit être effectuée la sauvegarde ?

- **Plutôt en local ou dans le cloud ou les deux ?**



Un mix des deux :

Il faut utiliser la règle des **3-2-1 :**

- Disposer de **trois** copies de vos données au minimum
- Stocker ces copies sur **deux** supports différents
- Conserver **une** de vos copies hors site.

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Par trois copies on entend : la source de vos données et 2 autres sauvegardes. Plus il y aura de copies, moins il y aura de risques de perte

Concernant les supports différents : ne pas mettre la sauvegarde sur le même périphérique que les données principales, au risque de perdre définitivement toutes les données en cas de panne de ce matériel

Pour la copie hors site : pour des raisons évidentes en cas d'incendie, vol, dégâts des eaux,…

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Une sauvegarde locale

Avantages :

- La vitesse d'exécution de sauvegarde et de bande passante : réseau local plus rapide que la connexion internet et que l'hébergeur, donc le backup sera plus rapide

- La restauration des données : plus rapide que de retélécharger toutes les données via la connexion internet

- Possibilité de mettre en place plusieurs sauvegardes locales différentes, grâce à la rapidité d'exécution

- Flexibilité du choix et du type de sauvegarde

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Inconvénients :

- Le vol physique du serveur et par conséquent des sauvegardes aussi
- Le risque d'incendie
- Le risque de piratage de la sauvegarde si le réseau n'est pas bien protégé (avec des firewalls, VLAN, etc.)
- Les pannes matérielles s'il n'y a pas de système redondant
- La maintenance et le renouvellement du matériel de sauvegarde est à anticiper et à planifier

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Conseils :

Isolez physiquement la solution de sauvegarde local de la source de données :

- dans des pièces différentes et à distance suffisante
- sur une autre protection électrique (onduleur)

Configurez des mots de passe différents pour l'accès à votre solution de sauvegarde physique

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Une sauvegarde dans le Cloud

Avantage :

La sécurité des données, placées en Datacenter sécurisé, grâce à plusieurs mécanismes :

- L'accès physique très limité et contrôlé
- La sécurité est renforcée
- Alimentations électriques redondantes
- Des réplications automatiques de serveurs vers d'autres datacenter (en fonction de vos choix)
- Monitorings en temps réel avec des équipes 24H/24 7J/7 pour intervenir directement
- La capacité d'augmenter rapidement l'espace de stockage
- Il y a des systèmes d'extinction automatiques d'incendie

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Inconvénient :

La vitesse de transfert dépendra de votre connexion internet

Conseils :

- Anticipez au maximum, le risque 0 n'existe pas !
- Rapprochez-vous d'une solution la plus sûre possible, mieux vaut utiliser un mix des deux sauvegardes locale et cloud.

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

- ***Sur quel type de support physique ?***

- **Disque dur ou clé USB** : contraignant et peu fiable comme unique sauvegarde en terme matériel, sécurité, dans la durée, le facteur humain.
- **Serveur NAS (Network Access Storage)** : backup via le réseau local, contient un ou plusieurs disques, petit système d'exploitation qui tourne dessus :
  - Choix de modèles variés : avec un ou plusieurs disques internes. Exemple : en RAID1 Miroir (en copie l'un de l'autre en cas de défaillance d'un disque)
  - Possibilité de dupliquer ses serveurs et d'avoir un MASTER et un SLAVE : un serveur principal et l'autre en copie permanente de celui-ci
  - Possibilité d'ajouter des disques de plus grande capacité pour suivre votre évolution, pas d'obligation de remplacer le serveur NAS.

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

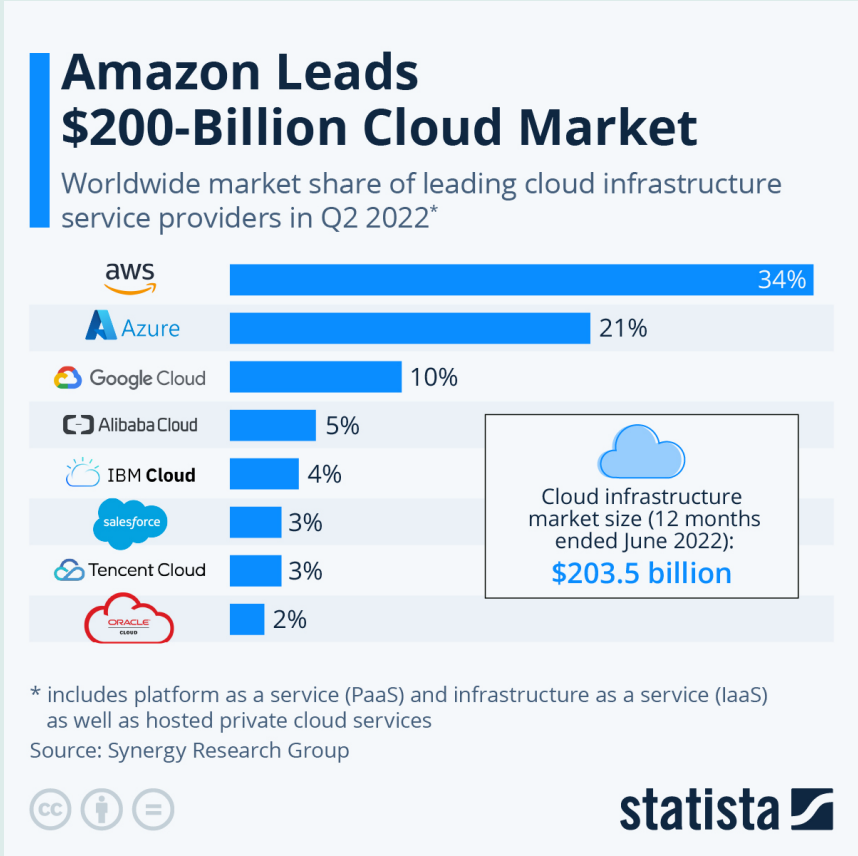
Exemple de serveur NAS : Synology

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

- ***Sur quel hébergeur Cloud de données ?***

3 leaders Cloud, tout service confondu :

- Amazon AWS :
  - Amazon S3 Glacier
  - Amazon Elastic File System (EFS)
  - AWS Simple Storage Service (S3)
- Microsoft Azure Storage :
  - Azure Archive Storage
  - Azure Blob Storage
  - Azure Disk Storage/Azure Files
- Google Cloud :
  - Cloud Storage Archive
  - FileStore
  - Cloud Storage



HelpIT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Attention :

- Le coût à la récupération peut être élevé en cas de restauration de sauvegarde

- Certaines solutions imposent un délai avant de pouvoir récupérer les fichiers

- Cryptez les données envoyées dans le cloud par sécurité et par confidentialité : un pirate ne pourra pas exploiter les données sans la clé de décryptage

- Externalisez un backup en dehors de l'environnement 365, configurez et optimisez les options du Tenant

HelpiT

NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

3. Quand et à quelle fréquence effectuer vos sauvegardes ?

- Le soir et/ou le week-end : lors de modifications minimum (voire aucune) des données

- Dépend du type des données et de la criticité :

  - Si modification régulière d'énormément de données, par jour et par heure : envisagez une première sauvegarde en continue

  - Prendre en considération le temps acceptable pour la perte de données entre deux sauvegardes

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

- Au minimum, une sauvegarde par semaine + une sauvegarde par soir

- Ajouter une sauvegarde mensuelle avec rétention de plusieurs mois + une sauvegarde annuelle à « archiver » en la déconnectant et en l'isolant de la solution de sauvegarde, afin qu'elle ne soit plus piratable ou altérable.

Attention de bien crypter ces données pour protéger du vol !

Le but est d'optimiser au maximum vos chances de récupération sur les fichiers les plus importants !

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

4. Renforcer son système, c'est aussi anticiper la restauration des données. Quel système de restauration des données privilégier ?

Après la mise en place de la méthode de sauvegarde, procéder à plusieurs tests :

1. Vérifier si le choix est correct ou s'il faut faire des adaptations.
2. S'assurer que les données soient réellement sauvegardées et accessibles. Ne pas se baser sur un simple rapport par mail.
3. Déterminer le temps de récupération nécessaire en condition réelle : la restauration via un serveur cloud peut parfois prendre plusieurs jours ou semaines dépendant de la quantité de données.
4. Vérifier ponctuellement si les données ne sont pas corrompues.
5. Comprendre votre mécanisme de restauration (faut-il aller chercher les données à plusieurs endroits ou dans une seule sauvegarde ?). Il est important de maîtrise et comprendre votre restauration.

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

Conseils :

- Prendre des notes sur la manière dont les sauvegardes sont configurées et sur comment procéder à la restauration.

  Aller plus loin : réaliser un **Business Continuity Plan** qui détaillera la totalité du processus.

- Le fait de réaliser ces tests permettra de déterminer également ou aller chercher en priorité les données : soit sur un support physique local, soit dans l'espace cloud.

HelpiT
NOUS PRENONS SOIN DE VOTRE INFORMATIQUE

01 02 03

Retour d'expérience : quels systèmes de sauvegarde ont été mis en place à la Ville de Liège ?

Benoit Joseph

Ville de Liège

Plan de présentation

- Les backups, pour se prémunir de quoi ?
  - Focus sur les « nouveaux » risques
- Eléments importants
  - Focus sur le « stockage immuable »
  - Focus sur les stockages dans le cloud
- Stratégies de backup
  - 3, 2, 1 (0)
  - GFS (Grandfather – Father – Son)
- Cas pratique

Les backups, pour se prémunir de quoi ?

- « Historiquement »
  - Se prémunir de la perte d'un serveur ou d'un centre de données
    - Notion de reprise après sinistre (potentiellement total)
  - Pouvoir restaurer une version antérieure
    - À la demande d'un utilisateur, …

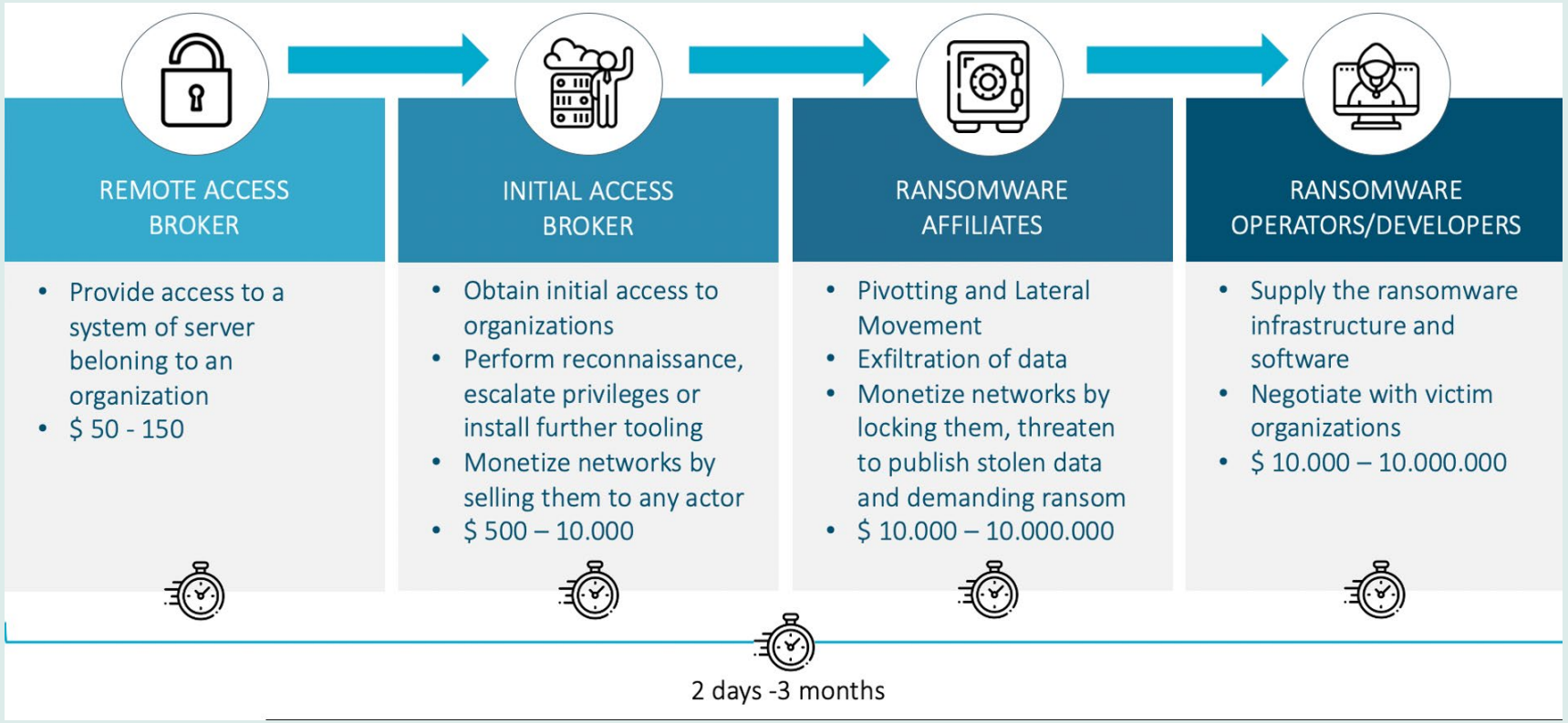
Les backups, pour se prémunir de quoi ?

- Aujourd'hui s'ajoute le point suivant
  - Augmenter la résilience pour faire face à une cyberattaque
    - Les ransomwares et cryptolockers en particulier

- Cette nouvelle menace implique de modifier l'approche historique

Focus : nouveaux risques - ransomware

- Schéma de l'attaque



Focus : nouveaux risques - ransomware

- Schéma de l'attaque
  - Mise en place entre 2 jours et 3 mois
  - Risque important que les backups soient corrompus à la source depuis un moment avant l'attaque
  - Risque important que les backups contiennent les éléments nécessaires à l'attaque

- Nécessité
  - De repenser les rétentions
  - D'assurer l'intégrité des sauvegardes
  - De tester régulièrement les backups
    - ce qui est de toute façon une bonne pratique

Eléments importants

- Le temps de restauration
  - Il est nécessaire d'estimer le temps nécessaire à restaurer une situation
    - En particulier dans le cas de stockage cloud
- La durée de rétention
  - Peut être fonction des données sauvegardées
  - Important dans le cas des ransomwares
  - A priori le plus et le plus longtemps on peut conserver est le meilleur
- Le matériel nécessaire
  - Stockage, serveur, réseau, …

Eléments importants

- Les ressources humaines nécessaires
  - Réalisation, suivi et test régulier des backups
  - Viser l'automatisation
- Les ressources financières
  - Souscription, espace de stockage cloud, consultance
- Définir sa stratégie pour répondre aux risques
  - Dans le cas d'un sinistre conséquent, l'assurance cyber peut perre la mise en œuvre de moyens exceptionnels
  - Ces moyens doivent être prévus et faire partie de la stratégie
    - Ex: restauration d'un gros volume de données à partir du cloud, certains prestataires offrent le rapatriement sur site sur une baie de disques louée

Eléments importants

- Principe de proportionnalité
  - Si les principes restent vrais, les moyens à mettre en œuvre sont fonction de l'institution
    - Sa taille, sa stratégie, le temps de restauration souhaité

- Les moyens doivent être mis en correspondance avec la stratégie établie
- Il en va de la continuité de l'institution

Focus sur le stockage immuable

- Principe
  - Les données ne peuvent être ni altérées ni supprimées par qui que ce soit, pour quelque raison que ce soit
    - Pour une durée définie

- Peut être implémenté sur différents supports
  - Disques, SSD, tapes, **cloud**

Focus sur le stockage immuable

- Applications et avantages clés du stockage immuable
  - Protège contre les ransomwares et autres cyberattaques
    - Si les backups n'ont pas été compromis à la source
  - Interdit les menaces internes malveillantes ou accidentelles
  - Permet de respecter les politiques de conformité réglementaire
  - Préserve l'authenticité des données

Focus sur le stockage immuable

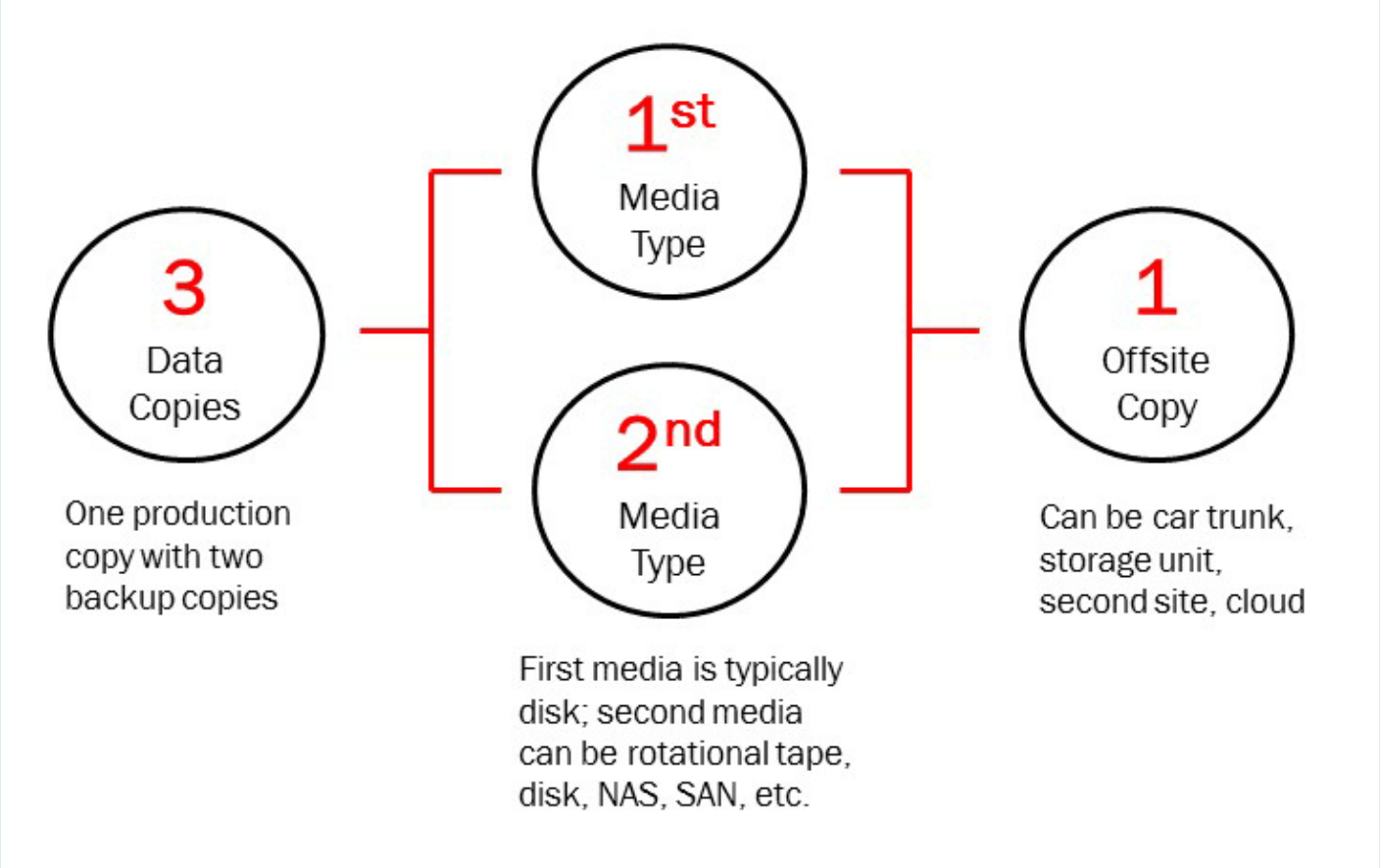
- Implémentations diverses
  - Logicielles
    - MinIO, système de fichiers Linux (XFS, ext4, BTRFS avec support des attributs étendus), Swarm
  - Matérielles
    - Inclut dans les NAS et SAN (ex: netApp, Dell/EMC, …)
    - Technologies optiques
  - Cloud
    - Amazon S3/Glacier, Azure blob, …

Focus sur les stockages Cloud

- Avantages
  - Permet d'externaliser une copie des backups
  - Permet d'implémenter le stockage immuable et de gérer la rétention
  - Pas d'infra à gérer
  - Pay as you use

- Inconvénients
  - Restauration potentiellement longue
    - Prévoir le rapatriement par baie de disque
    - Prévoir la possibilité d'augmenter la bande passante
      - Une assurance cyber peut couvrir ce type de coût
  - Coût de fonctionnement potentiellement important
    - Lectures, écritures, stockage, … les coûts dépendent des fournisseurs
    - Planification nécessaire

Stratégies de backup – 3 2 1 (0)



Stratégies de backup – 3 2 1 (0)

- Principe (minimum)
  - Avoir 3 copies
  - Sur 2 médias différents
  - Dont 1 hors site

- Idéalement
  - 0 inconsistance dans les backups
  - 2 copies hors site dont une offline

Stratégies de backup – GFS

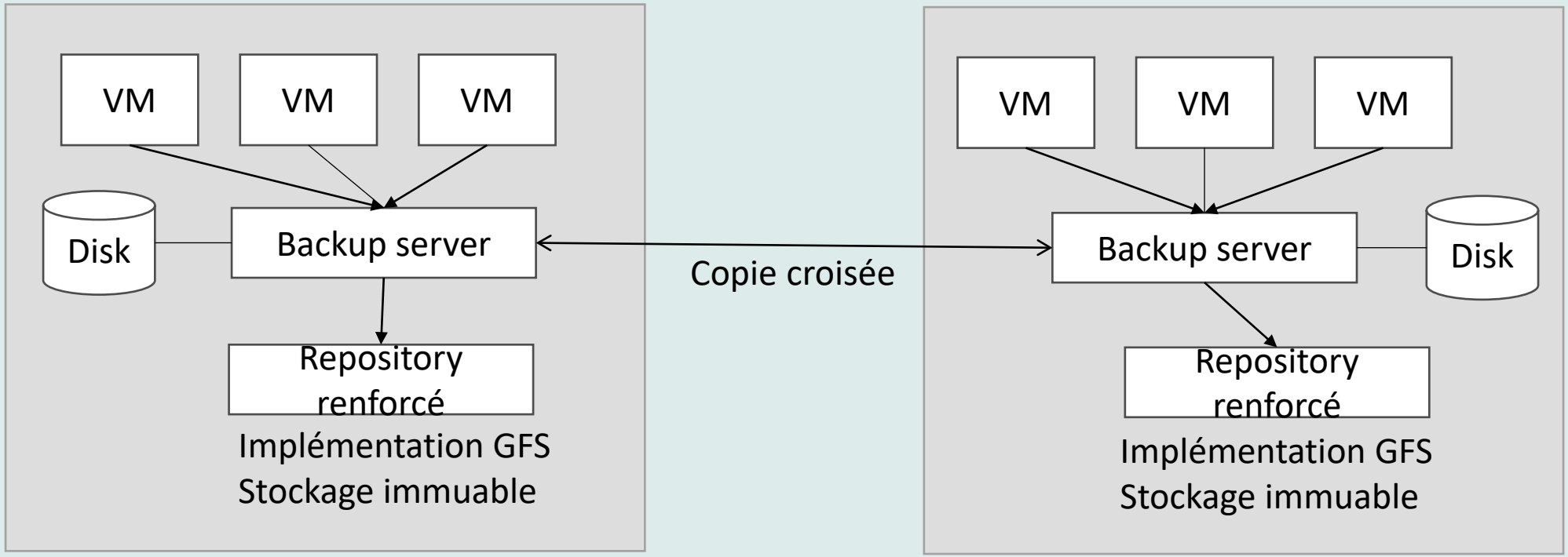
- GFS = Grandfather, Father, Son
- Principe
  - Schéma de rotation basé sur 3 cycles de backup ou plus
  - Ex: hebdomadaire, mensuel, annuel
- Une période de rétention peut être définie sur chaque cycle
- Peut être hors site
- Peut être stocké de manière immuable

Cas pratique – Ville de Liège

- Contexte
  - Infrastructure massivement virtualisée
  - Deux sites distants
  - Utilisation du logiciel de backup Veeam

Cas pratique – Ville de Liège

- Implémentation



Cas pratique – Ville de Liège

- Implémentation de 3 2 1
  - Plus de 3 copies
  - Sur 2 sites distincts
  - 1 hors site

- Implémentation de GFS
  - Cycle hebdomadaire, mensuel et annuel
  - Backup longue durée

Cas pratique – Ville de Liège

- Utilisation de Veeam
  - Solution complète et adaptée à la virtualisation
  - Facilite la mise en place des différentes stratégies et concepts
  - Offre de la compression et de la déduplication pour réduire les besoins en stockage

- Projet d'ajouter une copie cloud
  - Renforcer le caractère immuable
  - Renforcer le hors site et hors infrastructure

- Projet d'ajouter un contrôle systématique de la qualité des backups
  - Avec Veeam SureBackup

01 02 03

Centrale d'achats « cybersécurité » : quel accompagnement d'iMio aux pouvoirs locaux wallons ?

Olivier Collet

iMio

iMio en valeurs

- Intégrité et éthique
- Ouverture et transparence
- Coopération
- Maîtrise
- Innovation
- Efficacité et qualité

La centrale d’achats

- Audits (en cours) - Risques
- Mesures de sécurité - 2023

Les principes

- Une centrale d’achat établie sur base d’un accord-cadre par procédure ouverte
- Basé sur recommandations CCB (BISG) et ASD
- Mesures découlant des audits

Pour aller plus loin…

Nos webinaires en replay : nouvelles technologies
https://www.uvcw.be/formations/webinaires

Espace « e-gov, TIC et simplification administrative » - Site UVCW
https://www.uvcw.be/e-gov/accueil

Votre espace eCampus
Procédure de connexion :
https://vimeo.com/518713611/f3c95176c9

Nos formations « Management de la donnée »
https://www.uvcw.be/formations/list/data

Merci pour votre participation !

À bientôt !