Cybermenaces : comment protéger efficacement mes données ?

La tribune du Technopole
45 mn pour s'informer

Intervenant

Sébastien HEITZMANN
Gérant – RSSI - Dir. technique
KIWI BACKUP

/sheitzmann

2le@2le.net

Kiwi Backup
L'intelligence de la sauvegarde

SOMMAIRE

- Quels risques pour mes données en 2022 ?
- Les causes des pertes de données
- Quels moyens de protection pour les données ?
- La sauvegarde, l'assurance vie de mes données
- Questions/réponses

Quels risques pour mes données en 2022 ?

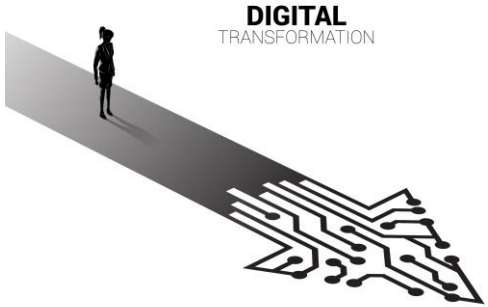
Etat des lieux

- **+ 300% des attaques par ciblage opportuniste** en 2021 (NTT Global Threat Intelligence)
- Explosion du nombre de **vulnérabilités 0-day exploitées** en 2021 (ANSSI)
- **Coût de la cybercriminalité** : 1000 milliards de dollars / an (Assureur Swiss Re)
- **22% des violations de données** signalées ont commencé par un **e-mail de phishing**

Etat des lieux

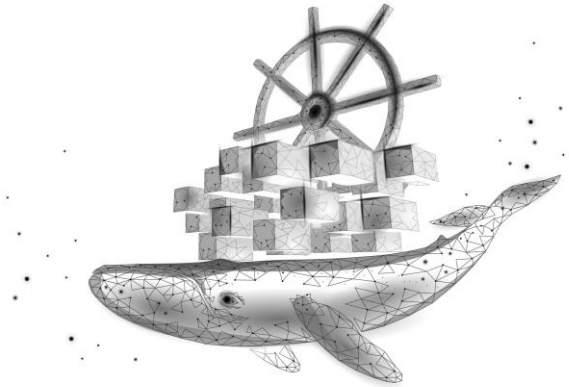
- **+ 37% d'intrusions avérées** dans les SI en 2021 (ANSSI)
- **+ 400% de tentatives de phishing** entre mars 2020 et mars 2021 (ANSSI)
- **8e place des pays les plus touchés par les cyberattaques** en 2020 (devant l'Allemagne, mais derrière la Grande-Bretagne et les Etats-Unis) (NTT Global Threat Intelligence)
- **Part dédiée à la cybersécurité sur le budget informatique** : 6,1 % en moyenne

Augmentation de la vulnérabilité : pourquoi ?



Nouveau usages numériques, digitalisation accélérée

Spécialisation et professionnalisation des attaquants



Complexification des architectures (Virtualisation, Docker)

Qui sont les cyberattaquants ?

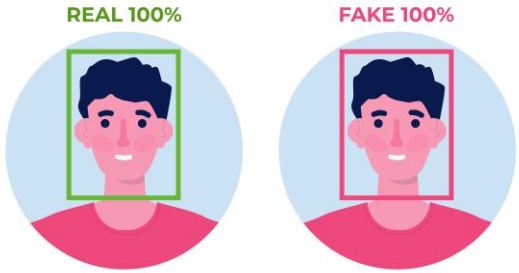
- **Script kiddies**
- **Cyberattaquants réputés étatiques** s'inspirant des méthodes et outils des cybercriminels classiques
- **Entreprises privées spécialisées** mettant sur le « marché » des outils performants et ergonomiques

Types d’attaques

Phishing

Attaque au président

Attaques DDoS



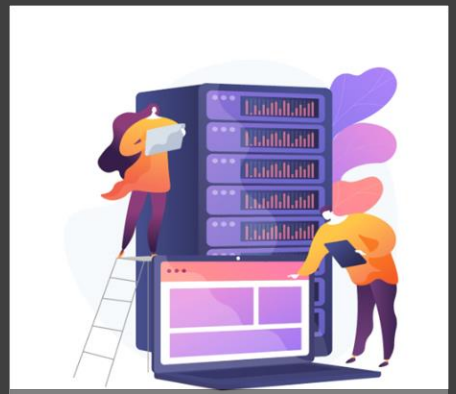
Deepfake

Spywares

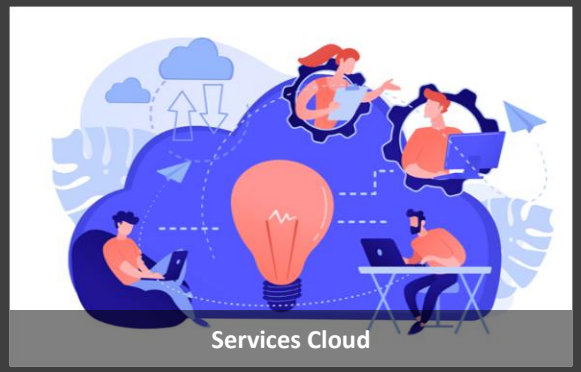
Ransomwares

Quelles cibles privilégiées en 2022 ?

Infrastructures critiques



Infrastructures cloud sous Linux

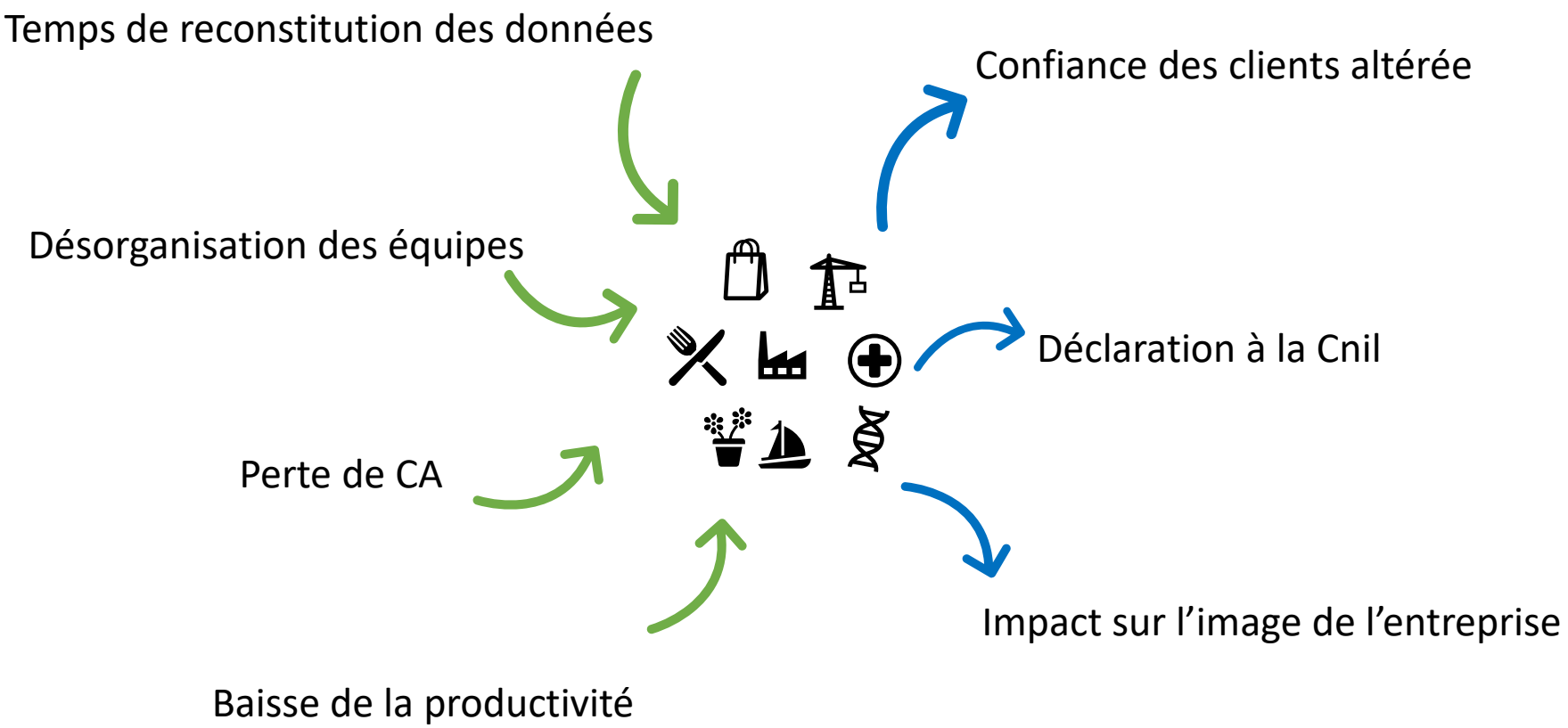


Services Cloud

Mondes virtuels

Supply Chain

Conséquences de la perte de données pour une organisation



Changement de dimension

« *Les attaques récentes sont des pré positionnements pour les conflits de demain, avec des groupes très organisés et probablement soutenus par des États. Ils mettent des charges dans les systèmes d'information en prévision d'un conflit. Un peu comme si on mettait de la dynamite sur les piliers des ponts en attendant la guerre* ».

Guillaume Poupard, le directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information)

Les causes des pertes de données

Causes de pertes de données

Internes

- Imprudence
- Mauvaise manipulation
- Manque de formation des collaborateurs
- Partage mot de passe
- Mot de passe faible ou volé

Erreur humaine

- Vétusté du matériel
- Mise à jour non faites
- Anti-virus
- Mauvais paramétrage firewall

Défaillance du matériel

Externes

- Cambriolage
- Incendie
- inondation

Cause naturelle

- Ransomwares
- Failles de sécurité
- Emails (phishing)
- Logiciels malveillants

Cybercriminalité

Les failles humaines

⇒ **63** % des incidents proviennent d'un collaborateur

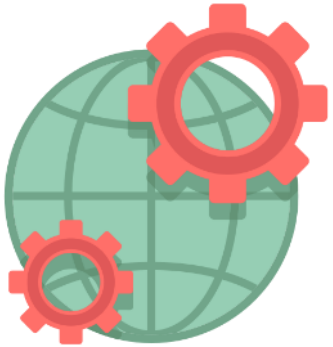
⇒Ils ne sont généralement pas assez formés aux risques et à la détection des attaques

⇒Ils ont souvent accès à des informations sensibles dans l'entreprise.

Les failles techniques

Postes de travail

Serveurs



Réseaux

- Laissent passer les différents virus
- Le matériel subit les risques de vols, d'incendie, d'usure, …

Quels moyens de protection pour les données ?

Vos données :
comment y voir clair ?

Réalisez une cartographie de vos systèmes et des données

- Quels logiciels utilisez-vous ?
- Quels types de données avez-vous ?
- Qui a accès aux données ?

Réalisez une cartographie des risques

- Où sont stockées vos données sensibles ?
- Quels sont les problèmes de sécurité éventuels ?

Quelles priorités
pour protéger ses données ?

- 3 thèmes sur lesquels travailler :

Organisation

Facteur humain

Technique

Actions organisationnelles

Organisation

- Créez une **charte** de sécurité informatique
- Mettez à jour les **habilitations**
- Réalisez une **procédure** des entrées et des sorties du personnel
- Vérifiez la bonne mise en place des **procédures et des actions**

Contre :

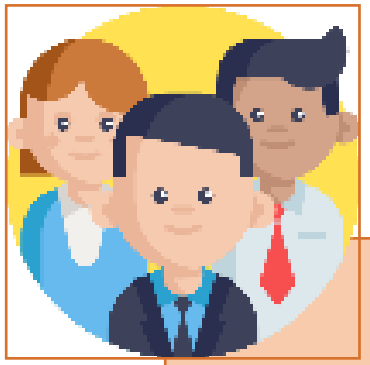
Phishing

Attaque au président

Ransomwares

Spywares

Actions « équipe »



Facteur humain

- Réalisez une **formation de sensibilisation** avec les nouvelles procédures
- Formez les employés à la **détection des phishings**
- Faire signer la **charte de sécurité**
- Mettez en place la **double authentification** (A2F)
- Mettez en place le **verrouillage automatique** des postes
- Mettez en place une politique pour le téléchargement des logiciels (liste des **logiciels autorisés**)
- Réalisez des **quizz** sur les phishings
- **Limitez la connexion** des supports mobiles
- Faire des **mises à jour** régulière

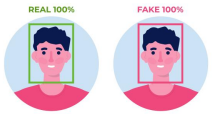
Contre :

Phishing

Attaque au président

Ransomwares

Spywares



Deepfake

Sensibilisation aux phishings : quizz et tests

Test de Google

https://phishingquiz.withgoogle.com/

Test Safeonweb

https://www.safeonweb.be/fr/participation/add/55

Test Phishingbox

https://www.phishingbox.com/phishing-test

Test bnz.co

https://www.bnz.co.nz/personal-banking/everyday-banking/keep-yourself-safe-online/phishing-quiz

Test accellis

https://accellis.com/email-phishing-quiz/

Les vidéos de la Hack Academy

https://youtu.be/lRqT3PtxA0Q

Actions techniques

Technique

- **Sauvegardez** vos données
- Faites les **mises à jour** de vos systèmes
- Installez un **anti-virus**
- Installez un **pare-feu**
- Limitez les ouvertures avec un bon **firewall**
- **Monitorez** vos serveurs
- **Loggez** les accès admin
- Configurez le **serveur de mail** pour empêcher le relais d'e-mail
- **Authentification** multi-facteurs (A2F)

Contre :

Phishing

Ransomwares

Spywares

Attaques DDoS

Pour aller plus loin

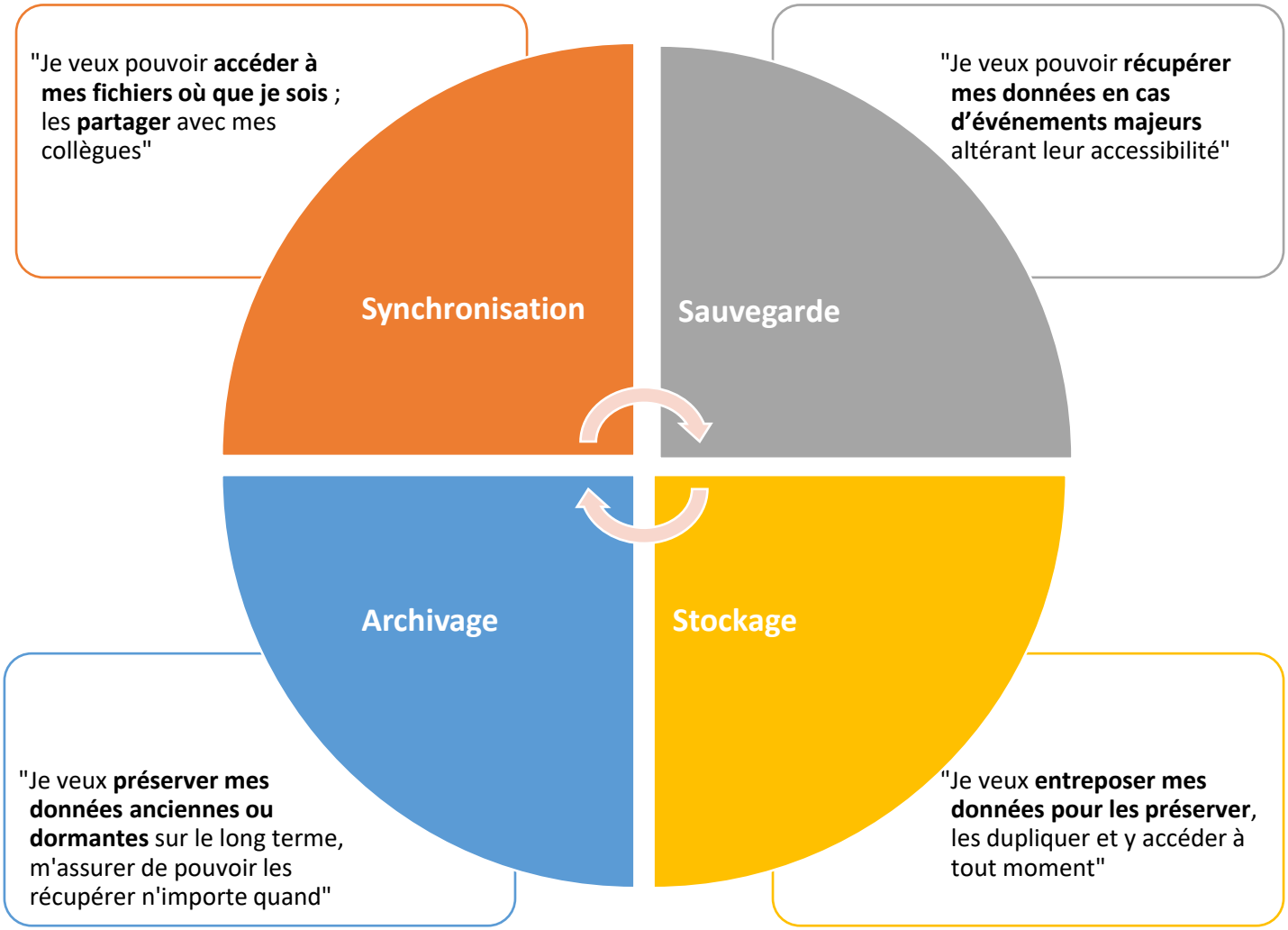
- **Cyber-résilience**
  - **Stocker** pouvoir assurer le minimum vital pour l'activité avec les données vitales sur des supports déconnectés
  - Avoir les moyens de **relancer** une application en mode dégradé
  - **Former** les collaborateurs et mettre en place les **procédure** pour des moyens manuels

Pour aller plus loin

- Ne pas oublier
  - S'exercer à la **réaction en cas d'attaque**
  - **Test PCA/PRA** avec simulation de cyberattaque majeure destructive (perte de données critiques) ou d'atteinte grave aux infrastructures (réseau, gestion des accès, gestion du parc,…) ➔ ex : pas de postes de secours / sauvegarde sur la même infra que la prod

La sauvegarde, l'assurance vie de mes données

Zoom sur la gestion des données



Kiwi Backup
L'intelligence de la sauvegarde

La sauvegarde c’est :

- Une obligation légale « *Le responsable du traitement est tenu de prendre toutes précautions utiles … pour* ***préserver la sécurité des données*** *et, notamment, empêcher qu'elles soient déformées, endommagées* »

  (Article 121 de la loi du 6 janvier 1978 du code pénal)

- Une sauvegarde **certifiée HDS** (hébergement données de santé) lors de l’externalisation des données médicales.

Eléments à prendre en compte pour choisir son système de sauvegarde

La sauvegarde doit permettre de remonter suffisamment loin en arrière dans le temps.

La sauvegarde ne doit pas pouvoir être altérée par le système.

Est-ce que mes données sont sures en cas d'incendie, inondation, …

Est-ce que l'on sauvegarde bien l'ensemble des données nécessaire à la reprise ?
Comment s'assurer d'avoir tous les éléments sauvegardés ?
Comment s'assurer de l'intégrité des sauvegardes ?

Est-ce que la sauvegarde fonctionne correctement tous les jours ?
Comment s'en assurer ?

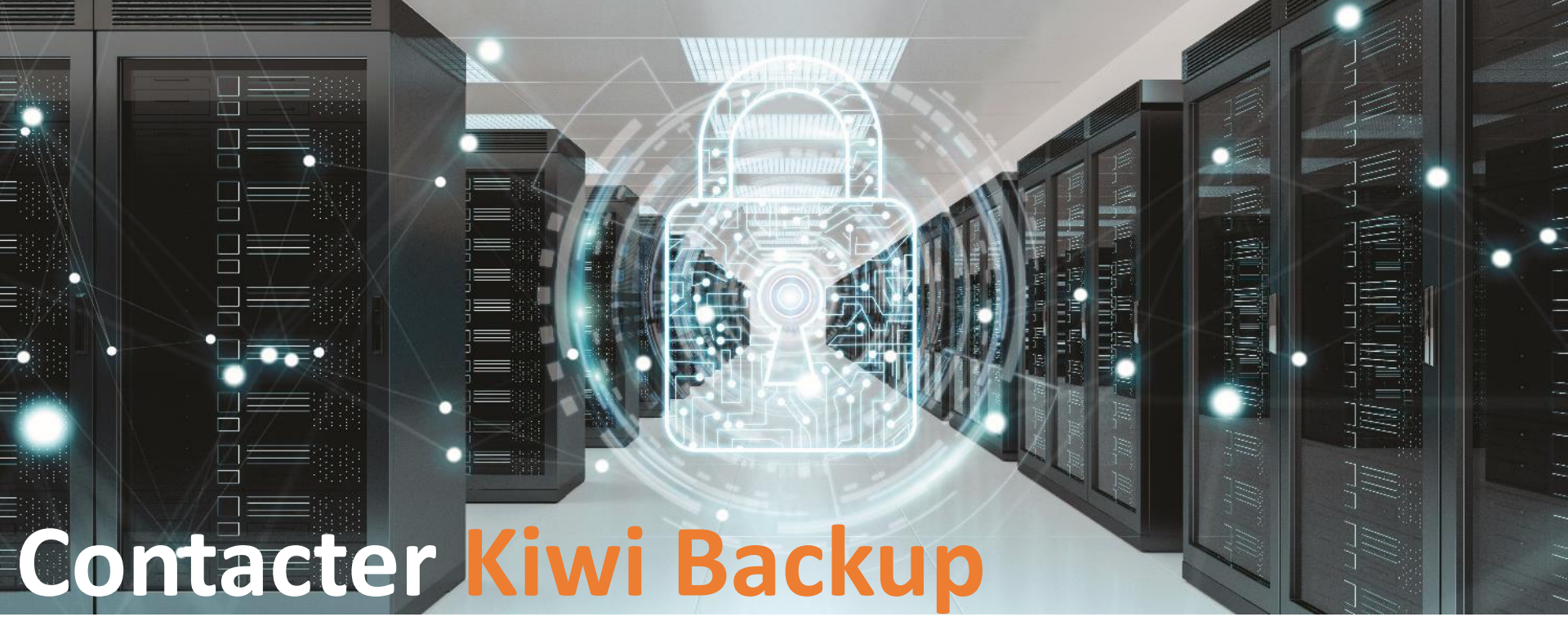
Kiwi Backup
L'intelligence de la sauvegarde

Quelques systèmes de sauvegarde passés au crible

Supports	Historique	Effectivité	Non altération	Externalisation
Clé USB	Non	Non	Oui/Non	Oui/Non
Disque dur externe	Non	Non	Oui/Non	Oui/Non
Serveur NAS	Non	Non	Oui/Non	Non
Bande	Oui	Oui	Oui	Oui/Non
Online	Oui	Oui	Oui	Oui
FTP	Oui/Non	Oui	Oui	Oui

La sauvegarde de données externalisée avec un historique long (90 à 365 jours) est la solution la plus fiable.

Questions/réponses



Contacter Kiwi Backup

Stéphanie MEYER

03 89 333 888

stephanie@kiwi-backup.com

Sébastien HEITZMANN

2le@2le.net

/kiwibackup /kiwibackup /kiwibackup