Les *Back Up*

Par Patrick Sentinel – 29a.ca

Cybersécurité : Le jour où vous remercierez votre backup (et regretterez de ne pas l'avoir testé)

Parlons sérieusement… Imaginez ceci : il est lundi matin, vous ouvrez votre ordinateur, café à la main, prêt à affronter une nouvelle semaine… et là, horreur. Tous vos fichiers portent des noms étranges, accompagnés d'un gentil message en anglais cassé :

"Your files is encrypted. Pay 3 bitcoin for decrypt. Have a nice day."

Voilà. C'est le moment où votre cœur s'arrête…

Mais si vous avez un **backup fonctionnel**, restaurable **vite et bien**, ce moment de panique peut se transformer en un simple :

"Ouf. On restaure notre crap, et on en parle plus."

Sinon, eh bien… vous apprenez le prix réel du mot *"dommage collatéral"*. Et, vous êtes dans les problèmes pour au moins une semaine au MINIMUM GARANTIE (pas de back up prêt = trouble assuré).

Un backup, ce n'est pas une archive poussiéreuse

Beaucoup voient les sauvegardes comme un vieux disque dur au fond d'un tiroir, jamais branché depuis Noël 2019. Mauvaise nouvelle : ce n'est pas une sauvegarde, c'est une **capsule temporelle**.

Un **vrai backup**, c'est :

- Régulier (quotidien idéalement, ou au moins selon un cycle adapté à votre rythme);
- Sécurisé (chiffré, hors ligne ou hors site);
- Testé (parce que "je pense que ça marche" est une réponse qui fait frémir… Sérieusement, si c'est votre réponse je vais devoir vous parler).

Les pires moments pour découvrir que votre backup est inutile

1. **Après une attaque par ransomware** : Surprise, le malware a chiffré vos fichiers ET votre disque de sauvegarde, connecté en permanence au système. Coup double.
2. **Après une panne matérielle** : Le serveur principal est grillé… et la seule sauvegarde est sur le même disque. Bien joué…. Fallait y penser avant!
3. **Pendant une inspection de conformité** : Un auditeur vous demande de prouver que vos données sont récupérables. Vous commencez à transpirer comme un serveur *Apache* en surcharge.
4. **Après une erreur humaine** : "J'ai supprimé le dossier 'compta_2024' sans faire exprès." Pas grave… sauf si la sauvegarde la plus récente date de 2022 😬.

Les règles d'or du backup version cybersécurité

Voici le kit de survie de tout professionnel un tant soit peu sérieux :

1. 3-2-1 : la règle sacrée

- **3** copies de vos données
- **2** types de supports différents (disque, cloud ou autre…)
- **1** copie hors site (pour éviter que tout parte en fumée, littéralement)

2. Automatiser pour ne jamais oublier

Les sauvegardes manuelles, c'est comme les résolutions du Nouvel An : ça tient une semaine. Automatisez tout, et dormez mieux.

3. Tester vos restaurations

Faites régulièrement un *fire drill* : choisissez une sauvegarde au hasard et restaurez-la dans un environnement de test. Si ça ne marche pas, **vous préférez le découvrir aujourd'hui que le jour où tout tombe en panne**.

4. Séparer et protéger vos sauvegardes

Un backup connecté 24/7 au réseau est une cible facile. Utilisez un NAS isolé, un cloud sécurisé, ou du stockage froid. Et surtout, **chiffrez tout**. On ne protège pas une copie critique avec un mot de passe "1234".

Le facteur temps : aussi important que la sauvegarde elle-même

Avoir une sauvegarde, c'est bien.
Mais **pouvoir la restaurer rapidement**, c'est encore mieux, trust me!

Imaginez deux scénarios :

- Vous avez une sauvegarde complète mais il faut **3 jours** pour tout réinstaller, reconfigurer, re-tester;
- Vous avez une sauvegarde bien pensée, avec des scripts de restauration automatisés. Tout est opérationnel **en une heure**, wow!

Dans le monde des affaires, **chaque minute compte**. Perdre trois jours, c'est perdre des clients, de l'argent, et parfois la confiance des partenaires. C'est pourquoi on parle de :

- **RTO (*Recovery Time Objective*)** : combien de temps max votre entreprise peut survivre sans ses systèmes;
- **RPO (*Recovery Point Objective*)** : combien de données vous êtes prêts à perdre (ex. : 1h, 4h, 24h de travail).

Connaissez ces deux chiffres, et **ajustez votre stratégie de sauvegarde en conséquence**.

En résumé : le jour où tout plante… qui appelle-t-on ?

Pas *Ghostbusters*. Pas votre cousin qui "s'y connaît un peu en informatique".

Ce jour-là, **votre meilleur allié**, c'est **votre plan de sauvegarde**.

Alors faites-vous un cadeau :

- Vérifiez vos sauvegardes;
- Testez vos restaurations;
- Automatisez, chiffrez, multipliez.

Parce qu'en cybersécurité, il n'y a rien de plus triste qu'un professionnel qui dit :

"On avait un backup… mais il était corrompu."

Et si vous n'en avez pas encore, voici une citation à méditer (inspirée d'un célèbre proverbe IT) :

"Il y a deux types de personnes : celles qui ont perdu des données, et celles qui *vont* en perdre."