Sauvegardez !

Régulièrement, un accident qui entraine la perte de données importantes nous rappelle l'importance des sauvegardes. L'incendie du centre de données d'OVH à Strasbourg le 10 mars dernier a été particulièrement spectaculaire, car de nombreuses personnes et organisations ont été touchées, mais des incidents de ce genre sont fréquents, quoique moins médiatisés. Un ami vient de m'écrire pour me demander mon numéro de téléphone car il a perdu son ordiphone avec son carnet d'adresses, un étudiant a perdu son ordinateur portable dans le métro, avec tout son mémoire de master dessus, et met une petite annonce dans la station de métro, une graphiste s'aperçoit que son ordinateur, avec tous ses travaux dessus, ne démarre plus un matin, une ville a perdu ses données suite au passage d'un rançongiciel, une utilisatrice de Facebook demande de l'aide car son compte a été piraté et elle ne peut plus accéder à ses photos de famille… Des appels au secours sur les réseaux sociaux comme celui-ci ou celui-là sont fréquents. Dans tous ces cas, le problème était l'absence de sauvegardes. Mais c'est quoi, les sauvegardes, et comment faut-il les faire ?

Le principe est simple : une sauvegarde (*backup*, en anglais) est une copie des données effectuée sur un autre support. Le but est de pouvoir récupérer ses données en cas de perte. Les causes de perte sont innombrables : vol de l'ordinateur portable ou de l'ordiphone (ces engins, étant mobiles, sont particulièrement exposés à ces risques), effacement par un logiciel malveillant ou par une erreur humaine, panne matérielle. Les causes possibles sont trop nombreuses pour être toutes citées. Retenons plutôt ce principe : les données peuvent devenir inaccessibles du jour au lendemain. Même si vous n'utilisez qu'un ordinateur fixe, parfaitement sécurisé, dans un local à l'abri des incendies (qui peut vraiment prétendre avoir une telle sécurité ?), un composant matériel peut toujours lâcher, vous laissant dans l'angoisse face à vos fichiers irrécupérables. Ne pensons donc pas aux causes de perte, pensons aux précautions à prendre.

(Au passage, saviez-vous que Lawrence d'Arabie avait perdu lors d'un voyage en train un manuscrit qu'il avait dû retaper complètement ? Il n'avait pas de sauvegardes. À sa décharge, avant le numérique, faire des sauvegardes était long et compliqué.)

La règle est simple : il faut sauvegarder ses données. Ou, plus exactement, **ce qui n'est pas sauvegardé peut être perdu à tout instant**, sans préavis. Si vous êtes absolument certain ou certaine que vos données ne sont pas importantes, vous pouvez vous passer de sauvegardes. À l'inverse, si vous êtes en train d'écrire l'œuvre de votre vie et que dix ans de travail sont sur votre ordinateur, arrêter de lire cet article et aller faire tout de suite une sauvegarde est impératif. Entre les deux, c'est à vous de juger de l'importance de vos données, mais l'expérience semble indiquer que la plupart des utilisateurices sous-estiment le risque de panne, de vol ou de perte. Dans le doute, il vaut donc mieux sauvegarder.

Comment on sauvegarde ?

Là, je vais vous décevoir, je ne vais pas donner de mode d'emploi tout fait. D'abord, cela dépend beaucoup de votre environnement informatique. On n'utilisera pas les mêmes logiciels sur macOS et sur Ubuntu. Je ne connais pas tous les environnements et je ne peux donc pas vous donner des procédures exactes. (Mais, connaissant les lecteurices du Framablog, je suis certain qu'ielles vont ajouter dans les commentaires plein de bons conseils pratiques.) Ensuite, une autre raison pour laquelle je ne donne pas de recettes toutes faites est que la stratégie de sauvegarde va dépendre de votre cas particulier. Par exemple, si vous travaillez sur des données confidentielles (données personnelles, par exemple), certaines stratégies ne pourront pas être appliquées.

Je vais plutôt me focaliser sur quelques principes souvent oubliés. Le premier est d'éviter de mettre tous ses œufs dans le même panier. J'ai déjà vu le cas d'une étudiante ayant bien mis sa thèse en cours de rédaction sur une clé USB mais qui avait la clé et l'ordinateur portable dans le même sac… qui fut volé à l'arrachée dans la rue. Dans ce cas, il n'y a pas de réelle sauvegarde, puisque le même problème (le vol) entraîne la perte du fichier et de la sauvegarde. Même chose si la sauvegarde est accessible depuis la machine principale, par exemple parce qu'elle est sur un serveur de fichiers. Certes, dans ce cas, une panne matérielle de la machine n'entrainerait pas la perte des données sauvegardées sur le serveur, en revanche, une fausse manœuvre (destruction accidentelle des fichiers) ou une malveillance (rançongiciel chiffrant tout ce qu'il trouve, pour le rendre inutilisable) frapperait la sauvegarde aussi bien que l'original. Enfin, si vous travaillez à la maison, et que la sauvegarde est chez vous, rappelez-vous que le même incendie peut détruire les deux. (Il n'est pas nécessaire que tout brûle

pour que tous les fichiers soient perdus ; un simple début de fumée peut endommager le matériel au point de rendre les données illisibles.) Rappelez-vous : il y a plusieurs causes de pertes de données, pas juste la panne d'un disque dur, et la stratégie de sauvegarde doit couvrir toutes ces causes. On parle parfois de « règle 3-2-1 » : les données doivent être sauvegardées en trois exemplaires, sur au moins deux supports physiques différents, et au moins une copie doit être dans un emplacement séparé. Bref, il faut être un peu paranoïaque et imaginer tout ce qui pourrait aller mal.

Donc, pensez à séparer données originelles et sauvegardes. Si vous utilisez un disque dur externe pour vos sauvegardes, débranchez-le physiquement une fois la sauvegarde faite. Si vous utilisez un serveur distant, déconnectez-vous après la copie.

(Si vous êtes programmeureuse, les systèmes de gestion de versions gardent automatiquement les précédentes versions de vos programmes, ce qui protège contre certaines erreurs humaines, comme d'effacer un fichier. Et, si ce système de gestion de versions est décentralisé, comme git, cela permet d'avoir facilement des copies en plusieurs endroits. Toutefois, tous ces endroits sont en général accessibles et donc vulnérables à, par exemple, un logiciel malveillant. Le système de gestion de versions ne dispense pas de sauvegardes.)

Ensuite, ne faites pas d'économies : il est très probable que vos données valent davantage que les quelques dizaines d'euros que coûte un disque dur externe ou une clé USB. Toutefois, il vaut mieux des sauvegardes imparfaites que pas de sauvegardes du tout. Simplement envoyer un fichier par courrier électronique à un autre compte (par exemple celui d'un ami) est simple, rapide et protège mieux que de ne rien faire du tout.

Enfin, faites attention à ce que la sauvegarde elle-même peut faire perdre des données, si vous copiez sur un disque ou une clé où se trouvent déjà des fichiers. C'est une des raisons pour lesquelles il est recommandé d'automatiser les sauvegardes, ce que permettent la plupart des outils. L'automatisation n'a pas pour but que de vous fatiguer moins, elle sert aussi à limiter les risques de fausse manœuvre.

« Five Days' Backup » par daryl_mitchell, licence CC BY-SA 2.0

À quel rythme ?

La règle est simple : si vous faites des sauvegardes tous les jours, vous pouvez perdre une journée de travail. Si vous en faites toutes les semaines, vous pouvez perdre une semaine de travail. À vous de voir quel rythme vous préférez.

Et le *cloud* magique qui résout tout ?

Quand on parle de sauvegardes, beaucoup de gens répondent tout de suite « ah, mais pas de problème, moi, tout est sauvegardé dans le *cloud* ». Mais ce n'est pas aussi simple. D'abord, le *cloud* n'existe pas : il s'agit d'ordinateurs comme les autres, susceptibles des mêmes pannes, comme l'a tristement démontré l'incendie d'OVH. Il est d'ailleurs intéressant de noter que beaucoup de clients d'OVH supposaient acquis que leurs données étaient recopiées sur plusieurs centres de données, pour éviter la perte, malgré les conditions d'utilisation d'OVH qui disaient clairement que la sauvegarde était de la responsabilité du client. (Mais qui lit les conditions d'utilisation ?)

Parfois, la croyance dans la magie du *cloud* va jusqu'à dire que leurs centres de

données ne peuvent pas brûler, que des copies sont faites, bref que ce qui est stocké dans le nuage ne peut pas être perdu. Mais rappelez-vous qu'il existe d'innombrables causes de perte de données. Combien d'utilisateurs d'un service en ligne ont eu la mauvaise surprise de découvrir un matin qu'ils n'avaient plus accès à leur compte parce qu'un pirate avait deviné leur mot de passe (ou détourné leur courrier ou leurs SMS) ou parce que la société gestionnaire avait délibérément fermé le compte, en raison d'un changement de politique de leur part ou tout simplement parce que le logiciel qui contrôle automatiquement les accès a décidé que votre compte était problématique ? Il n'est pas nécessaire que la société qui contrôle vos fichiers perde les données pour que vous n'y ayez plus accès. Là aussi, c'est une histoire fréquente (témoignage en anglais) et elle l'est encore plus en cas d'hébergement gratuit où vous n'êtes même pas un client.

Ah, et un autre problème avec la sous-traitance (le terme correct pour *cloud*), la confidentialité. Si vous travaillez avec des données confidentielles (s'il s'agit de données personnelles, vous avez une responsabilité légale, n'oubliez pas), il n'est pas prudent de les envoyer à l'extérieur sans précautions, surtout vers les fournisseurs états-uniens (ou chinois, mais ce cas est plus rare). Une bonne solution est de chiffrer vos fichiers avant l'envoi. Mais comme rien n'est parfait dans le monde cruel où nous vivons, il faut se rappeler que c'est moins pratique et surtout que cela introduit un risque de perte : si vous perdez ou oubliez la clé de chiffrement, vos sauvegardes ne serviront à rien.

Tester

Un adage ingénierie classique est que ce qui n'a pas été testé ne marche jamais, quand on essaie de s'en servir. Appliqué aux sauvegardes, cela veut dire qu'il faut tester que la sauvegarde fonctionne, en essayant une restauration (le contraire d'une sauvegarde : mettre les fichiers sur l'ordinateur, à partir de la copie).

Une bonne discipline, par exemple, est de profiter de l'achat d'une nouvelle machine pour essayer de restaurer les fichiers à partir de la copie. Vous serez peut-être surpris·e de constater à ce moment qu'il manque des fichiers importants, qui avaient été négligés lors de la sauvegarde, ou bien que la sauvegarde la plus récente n'est… pas très récente. Ou bien tout simplement que la clé USB où vous aviez fait la sauvegarde a disparu, ou bien ne fonctionne plus.

Conclusion

Il faut sauvegarder. Je l'ai déjà dit, non ? Pour vous motiver, posez-vous les questions suivantes :

- Si, un matin, mon ordinateur fait entendre un bruit de casserole et ne démarre pas, saurais-je facilement restaurer des données sauvegardées ?
- Si toutes mes données sont chez un hébergeur extérieur et que je perds l'accès à mon compte, comment restaurerais-je mes données ?
- Si je travaille sur un ordinateur portable que je trimballe souvent, et qu'il est volé ou perdu, où et comment restaurer les données ?

Si vous préférez les messages en vidéo, j'ai bien aimé cette vidéo qui, en dépit de son nom, n'est pas faite que pour les geeks.