IDCLIC
MAINTENANCE
INFORMATIQUE

BACKUP - CLOUD - VPN

Guide pratique

Frédéric Wauters
frederic.wauters@idclic.be

IDCLIC - Service de maintenance de *A idées formation asbl*
Boulevard des Archers 10 - 1400 Nivelles
Tél : 067 21 03 58 - 0487 65 43 72 - www.aid-formation.be - info@aid-formation.be
N° ent : BE 0472.750.086 – Tribunal des entreprises de Nivelles

Table des matières

Introduction

Gérer ses données, les mettre en sécurité ou encore y accéder en dehors de leur environnement habituel est un sujet entier qui demande une vraie analyse. Il ne faut pas se lancer à corps perdu à dans la mise en place d'une solution sans en avoir étudié tous les aspects.

Au cœur de la multitude des systèmes et des outils existants, comment s'y retrouver ? Quelle sont les différences entre toutes ces solutions et surtout, comment faire le bon choix ? Quels investissements y consacrer ? Que valent les solutions bon marché ou gratuites ? Comment être certain de ne pas se tromper, de ne pas déployer énergie et argent à une solution non adaptée ?

Cloud, backup : définitions

Parmi les différentes technologies qui rythment notre quotidien numérique, il est parfois difficile de comprendre et de s'y retrouver. L'évolution de l'informatique et de ses moyens est tellement rapide qu'elle est parfois difficile à suivre. Nous vous proposons quelques éclairages.

1. Cloud, nuage

Nous entendons souvent ces deux termes, plus souvent « Cloud » que « Nuage » mais il s'agit du même mot (Cloud : nuage en anglais).

Le *Cloud* est un stockage distant, ceci signifie que vous stockez ailleurs vos données, vos fichiers, vos images, etc. Plutôt que d'enregistrer localement sur votre disque dur, votre clé USB ou encore votre serveur réseau, vous envoyez ces objets sur Internet, dans un espace qui vous est réservé et pour lequel vous disposez d'un accès sécurisé.

Généralement, les fournisseurs permettant les stockages en *Cloud* disposent d'énormes salles informatiques remplies d'armoires de serveurs (datacenter). L'utilisation du *Cloud* est également souvent appelée *Cloud computing*. Le terme *Nuage* quant à lui n'est guère utilisé qu'en France ou au Canada, et de manière assez rare.

Les fichiers du *Cloud* sont accessibles directement et à tous moments, il suffit de disposer des accès nécessaires.

2. Backup

Aussi appelé *Sauvegarde*, le *backup* permet de mettre à l'abri une copie de vos informations et fichiers les plus importants. Il peut s'agir de n'importe quel type de données. L'idée est de sauvegarder toutes les données indispensables sans lesquelles vos activités seraient mises à mal.

De nombreux fournisseurs proposent de sauvegarder vos données importantes sur leurs serveurs. De nouveau, il s'agit de salles informatiques immenses, regorgeant de serveurs impressionnants. Les données y sont enregistrées également via Internet et de manière aussi sécurisée.

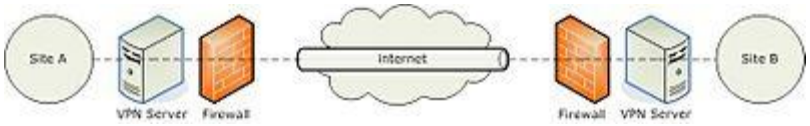
Il s'agit donc de copier dans cet espace de stockage distant les fichiers nécessaires et ce, de manière régulière. Le but étant de se protéger contre la perte de données locales ou le piratage (notamment par ransomware), il est évident que ceci doit se faire à fréquence soutenue.

Lors du transfert des données, un cryptage assure une sécurité des données tant vis-à-vis des pirates que du fournisseur de stockage.

3. Le VPN

Cet acronyme signifie *Virtual Private Network* qui signifie *Réseau Privé Virtuel*. A l'heure actuelle, le *VPN* est souvent utilisé pour éviter d'être localisé ou tracé lors d'actions illicites. Pour pouvoir télécharger des contenus de manière illégale, beaucoup utilisent cette méthode. Il s'agit avant tout d'une technique permettant d'isoler des ordinateurs qui doivent communiquer de manière sécurisée.

Pour ce faire, le *VPN* crée un « tunnel étanche » permettant ainsi de sécuriser les données par rapport au reste d'Internet.



Si vous êtes en possession d'un serveur (par exemple un NAS), il est souvent possible d'y installer un système *VPN* pour sécuriser vos données. Si votre serveur dispose déjà d'un système de type *Drive* pour l'accès permanent à vos données, il est certainement en mesure de crypter les informations sans avoir besoin d'installer un VPN. Cependant, l'accès à ces données à partir de réseaux publics comme des hotspots (points d'accès Wi-Fi publics) présente un risque et peut nécessiter l'installation de ce système.

Les *VPN* permettent l'accès de point à point (d'un ordinateur à un autre) ou en infrastructure (en réseau).

Une évolution intéressante de ce système est à explorer : le SD-LAN.

4. Le SD-LAN

SD-LAN est l'abréviation de *Software Defined Local Area Network*. Il s'agit d'un réseau informatique au même titre qu'un réseau local (Ethernet ou Wi-Fi) auquel peuvent se joindre des ordinateurs qui ne se trouvent pas physiquement à proximité du réseau. Il est géré de manière logicielle, généralement via une interface en ligne. Pour un réseau moyen, la société *ZeroTier* offre une solution gratuite et performante.

De cette manière, le gestionnaire peut décider d'ajouter les différents utilisateurs à l'un ou l'autre ou plusieurs de ses réseaux. La gestion se fait en temps réel et nécessite l'installation d'un petit logiciel sur chaque ordinateur du réseau. Si vous disposez d'un serveur, il faudra également lui ajouter ce logiciel pour l'intégrer aux réseaux nécessaires.

À l'aide de ce système sécurisé, un employé peut accéder aux données de son entreprise auxquelles il a habituellement accès sans devoir utiliser un autre système. Nombre de ces infrastructures utilisent une base *VPN* pour permettre la création de ce type de réseau.

Le *SD-LAN* a pu être testé au sein de l'*A idées formation* durant le confinement de 2020 avec succès.

Les différences

Il est compréhensible, au vu des définitions ci-avant, que la confusion ait tendance à s'installer, surtout pour un néophyte. Quelles différences caractérisent notamment le *Cloud* et le *Backup* ? C'est d'autant plus vrai que, lors d'un backup distant, vous entendrez parler de *Backup dans le Cloud* !

Pour être bref, nous dirons que le *Cloud* sera plutôt utilisé comme serveur de fichier pour le travail au quotidien. À titre d'exemple, *Dropbox, Azure, OneDrive, Synology Drive, Google Cloud* ou *Google*

Drive, sont des plateformes permettant ce type de fonctionnement. **Le principal avantage est que vous accédez à vos fichiers distants pour y travailler à tout moment et de n'importe où !**

Le *Backup* quant à lui est une sauvegarde permettant de restaurer une situation saine en cas de problème. Il ne s'agit pas ici de travailler directement avec ces fichiers. L'idée d'un backup est de dupliquer l'entièreté des données importantes de votre serveur local ou de votre ordinateur, Lorsqu'un problème sévère survient et altère vos données locales, vous pouvez les restaurer rapidement en partant du dernier *backup* réalisé. **C'est indéniablement la sécurité ultime pour être à l'abri des pertes de données !**

Contrairement au *Cloud*, les fichiers sauvegardés lors des backups sont cryptés et ne peuvent être lus directement. Dès lors, ce n'est pas une bonne idée d'y accéder à n'importe quel moment pour les retravailler. Même si cela reste possible, ce n'est pas sain et encore moins pratique. Généralement, ces données sont empaquetées et modifier un des fichiers implique qu'il faut d'abord rapatrier une quantité importante de données, modifier un fichier du paquet, refaire le paquet et le stocker à nouveau sur les serveurs. Avec le temps, les outils ont évidemment évolué et permettent l'accès à un fichier en particulier en cas de besoin. Mais ce n'est vraiment pas un système adapté à un travail direct sur les fichiers. Préférez dans ce cas le *Cloud*.

CLOUD	BACKUP 
Stockage distant	**Sauvegarde** distante
Accès « **direct** » sécurisé	Accès **bloc** crypté
Synchronisation possible (à chaque modification)	**Copie** en bloc (incrémentale possible)
Pas prévu pour **historiser** les changements (mais possible)	**Historisation** recommandée (plusieurs backups)
Disponibilité des mêmes fichiers sur **plusieurs appareils**	**Sauvegarde** de **plusieurs appareils** = **plusieurs backups**
Possibilité de verrouiller un fichier ouvert par un utilisateur	**Pas de verrouillage de fichier ouvert par un autre utilisateur**

Le *VPN* et le *SD-LAN* sont clairement différents du *Cloud* et du *backup*. Le *SD-LAN* étant basé sur le *VPN*, il n'est pas pertinent d'analyser les différences. Il faut cependant noter que le *SD-LAN* va plus loin et crée un tunnel sécurisé entre deux ordinateurs en émulant une couche réseau, permettant l'accès à l'ensemble d'un réseau facile à créer et à gérer.

La pollution numérique

Utiliser ces technologies génère une pollution numérique, nous en sommes bien conscients. Aussi, lorsque nous cherchons des solutions, nous prenons en compte la manière dont fonctionnent les services tiers que nous conseillons ou que nous utilisons.

Néanmoins, il est difficile de quantifier cette pollution supplémentaire et de la comparer à celle que nous générons quotidiennement en utilisant des services traditionnels. Par exemple, des scientifiques ont estimé la pollution numérique générée par les mails quotidiens, ils l'ont comparée à la pollution générée par le courrier papier. Il s'avère qu'un mail pollue six fois moins qu'un courrier papier. Par contre, la facilité offerte par le courrier électronique nous incite à envoyer soixante fois plus de mail que de lettres. La gestion de cette pollution numérique ne se fait donc pas uniquement du côté du fournisseur.

L'idée ici n'est pas d'entrer dans un débat sur l'enjeu écologique. **IDCLIC** garde un œil attentif sur les technologies utilisées par les services tiers mais également sur le type d'énergie utilisée ou générée. Certains fournisseurs sont quasiment autonomes en énergie (panneaux solaire, pompe à chaleur, etc.)

La sécurité

Qui dit accès de ou vers l'extérieur dit risque : vous avez raison ! Mais évidemment, ce point -vous vous en doutez- a été pris en compte. C'est pour cette raison que les transferts de données sont sécurisés.

1. Des données cryptées

Pour accéder à vos fichiers (que ce soit pour le *Cloud* ou pour le *backup*), vous devez bien entendu disposer de codes d'accès. Outre ce premier niveau de sécurité, les données sont cryptées à l'aide de clés. En toute logique, le fournisseur de stockage ne décide pas de ces clés, **ce sont les utilisateurs de ces stockages qui en décident.** Les services et logiciels clients permettant ces échanges se chargent automatiquement de générer les clés nécessaires à ceux-ci.

Sachez cependant que, même si votre service de maintenance informatique dispose de ces clés de cryptage, elles ne lui permettent que de mettre en relation vos données avec le fournisseur de stockage. Il est très difficile de décrypter les données même en ayant ces clés. Les appareils chargés des échanges sont dotés du nécessaire pour le faire. Toute personne qui souhaiterait pirater ces données même en ayant les clés devrait s'armer de patience et d'outils complexes.

2. Le RGPD

Malgré les cryptages décrits ci-dessus, **le *RGPD* est un aspect à ne pas négliger**. Il convient de se renseigner au préalable avant de choisir son opérateur de stockage. En effet, ce n'est pas parce que les transactions sont cryptées que le *RGPD* est respecté. Informez-vous pour mieux connaître votre opérateur. Il est par exemple important de **vérifier où seront stockées vos données et à quelle législation est soumis l'opérateur**. S'il respecte la législation hors Europe, il ne respecte peut-être pas le *RGPD*, il n'est peut-être pas tenu de le faire. Dans ce cas, **quelle garantie avons-nous quant au respect de la confidentialité de vos données ? Les données sont-elles bien en sécurité ?**

Cloud ou backup ? Que choisir ?

Vous connaissez à présent les différences entre les deux concepts, encore faut-il pouvoir choisir. Tout dépendra de votre infrastructure actuelle (et à venir).

1. Le cloud

Plusieurs raisons peuvent motiver ce choix. Par exemple, vous voulez accéder à tous vos fichiers n'importe où, dans ce cas, le *Cloud* est idéal. Il en est de même si l'ensemble de votre équipe doit collaborer sur ces mêmes fichiers. Notez d'ailleurs qu'en travaillant sur un fichier qui est synchronisé sur le *Cloud*, celui-ci n'est pas pour autant verrouillé. Un autre utilisateur peut le modifier en même temps. Mais les services qui gèrent le *Cloud* utilisent des techniques permettant d'éviter les conflits de versions.

D'autres raisons peuvent motiver ce choix. Par exemple, votre serveur devient trop vieux ou est parfois défaillant, c'est peut-être le moment de changer pour cette solution de remplacement. Vous me direz sans doute qu'en absence de connexion Internet, vous ne pourrez pas accéder à vos fichiers. C'est vrai, mais pas tout à fait. La plupart des fournisseurs de *Cloud* proposent un outil de synchronisation. Grâce à cela, les dossiers synchronisés apparaissent (comme n'importe quel

dossier du disque dur) dans votre explorateur de fichiers. Une copie locale des fichiers est présente physiquement sur votre disque dur. Vous travaillez toujours dans cette copie locale, que vous soyez connecté ou non à Internet. Lorsque vous récupérez une connexion, l'outil met à jour le *Cloud* avec les fichiers ainsi modifiés.

Notez que ce système n'a rien de commun avec un backup, ce serait une mauvaise idée d'en faire usage dans ce cadre !

2. Le backup

La principale utilisation d'un backup est de sauvegarder les données de votre serveur ou de vos ordinateurs sur un espace protégé. Il est important de considérer l'importance de vos données et d'en garder une copie en cas de « catastrophe ». Vous me direz peut-être que vous procédez déjà à des backups réguliers sur un disque dur externe ou des clés USB.

Nous ne pouvons que vous féliciter mais ce n'est malheureusement pas suffisant. Où stockez-vous vos backups ? Combien en avez-vous ? Sur quelle durée pouvez-vous remonter ?

Généralement, les backups restent au même endroit. Dès lors, en cas d'incendie ou de tout autre sinistre, les backups pourraient être perdus, inutilisables. Dans certains cas, il est important de remonter plusieurs jours en arrière et restaurer les données plus anciennes. Avec un seul backup sur disque dur externe ou clé USB, vous ne pourrez peut-être pas le faire. Quant à la fiabilité de ces appareils, vous n'avez que peu de garantie.

Les backups sur serveur distant vous permettent de restaurer des données sauvegardées plusieurs jours ou semaines ou mois en arrière. Tout ceci dépend, bien entendu, de la configuration de vos backups. En outre, votre opérateur de stockage dispose de sécurité supplémentaire évitant les avaries techniques des supports de stockage. La disponibilité des données est également mieux étudiée. Enfin, face à un sinistre physique de vos installations (incendie, inondation, etc.) votre backup distant est sain, à l'abri.

En matière de backup, il existe une règle appelée 3-2-1. Elle signifie qu'il faut disposer de 3 copies de vos données au moins, se trouvant sur 2 supports de types différents dont 1 ne se trouve pas au même endroit. Dès lors, si l'on désire être en sécurité, il ne suffit pas de disposer d'un backup local de vos données, il faut également disposer d'une copie ailleurs.

Par exemple :

- Disposer d'un serveur pour vos données (1ère copie **sur site**)
- Garder un backup sur site, par exemple sur disque dur externe (2ème copie **sur site**)
- Posséder un backup en ligne via Internet chez un opérateur adéquat (3ème copie **hors site**)

Les solutions disponibles

Les **hébergeurs** proposent (quasiment) tous des possibilités de *Cloud* et de *Backup*. Les outils de synchronisation existent aussi pour ces solutions mais pas chez chacun.

Certaines sociétés se sont spécialisées dans le *backup* de données en ouvrant les protocoles sophistiqués garantissant la sécurité des données et des fichiers.

Enfin d'autres sociétés se sont quant à elles spécialisées dans les *Cloud* offrant des outils de synchronisation généralement très corrects.

IDCLIC reste à votre disposition et vous aidera volontiers pour le choix et la mise en service de votre *Cloud* ou de vos *backups*. **N'hésitez pas à nous contacter !**

Quelle que soit la solution choisie, vérifiez toujours bien les points de sécurité évoqués plus haut. Vérifiez également s'il s'agit de contrats par utilisateur ou non. Les prix peuvent fortement varier. Nous vous proposons ci-après une liste non-exhaustive à titre d'exemple et comme première piste de recherche pour vous aider (prix hors TVA indicatif, non contractuel, prix au 16/10/2020) :

NOM	TYPE	Formule/taille/prix	Remarque
AL1FO	Backup	Pico / 250 Go / 6 € Méga / 500 Go / 9 € Téra / 1 To / 12 € Péta / 1,5 To / 15 €	Belgique/Allemagne RGPD Prix mensuel
pCloud	Cloud	Free / 10 Go / 0 € P500 / 500 Go / 60 € P2T / 2 To / 120 €	Luxembourg/Texas RGPD Prix annuel
Sync.com	Cloud	Standard / 1 To / 5 $ Plus / 4 To / 8 $ Advanced / 10 To / 15 $	Toronto RGPD Prix par mois par utilisateur
OneDrive	Cloud	BusinessBasic / 1 To* / 4,20 € BusinessStandard / 1 To* / 10,50 € * sous réserve d'éligibilité	Etats-Unis RGPD Prix mensuel par utilisateur
OVH	Backup	Standard 250 / 250 Go / 6 € Standard 1000 / 1 To / 13 € Stansard 2000 / 2 T0 / 23 €	France RGPD Prix mensuel
BlackBlaze	Backup	Formule unique (stockage illimité) 6 $	Etats-Unis et Europe (en utilisant partiellement les WebServices de Amazon)
Office 365	Cloud	Gratuit pour association (sous réserve d'éligibilité) Basic : 0 € Business standard : 2,50 €	Selon l'éligibilité, il est possible de disposer de plus ou moins de services gratuitement. Il s'agit d'études au cas par cas. RGPD

Il existe encore beaucoup d'autres fournisseurs. La liste ci-dessus se veut la plus diversifiée possible, tant au niveau du prix que des types de contrats. Il faut d'ailleurs prêter une certaine attention à ces diverses formules et bien calculer pour y trouver son propre avantage.

D'ailleurs, le prix n'est pas toujours l'élément le plus déterminant. **IDCLIC** attache une importance particulière au rapport qualité/prix mais également à l'aspect local. Le critère éthique et durable guide aussi nos choix.

Par exemple, **AL1FO** (première ligne du tableau) est un fournisseur belge basé à Grandrieu (Chimay). Ses serveurs se trouvent en Belgique et sont répliqués (redondance de sécurité) en Allemagne.

VPN, SD-LAN ? Est-ce nécessaire ?

Une fois encore, tout dépend de la mise en place que vous avez prévue. Si vous décidez de tout déplacer dans le *Cloud*, il semble évident que le *VPN* ou le *SD-LAN* ne vous servira à rien. Si vous décidez de garder votre serveur ou d'évoluer vers un nouveau et que vous utilisez un système *Drive* intégré à ce serveur, le *VPN* et le *SD-LAN* ne s'appliquent pas non plus.

En revanche, si vous ne souhaitez utiliser ni *Drive*, ni *Cloud* (ou pas totalement), le *VPN* ou le *SD-LAN* sont des solutions très intéressantes. Pour l'avoir testé sur notre site, le *SD-LAN* semble plus intéressant que le *VPN*.

Que vous utilisiez le *VPN*, le *SD-LAN* ou pas, ne remet pas en cause la nécessité d'implémenter un système de *backup* pour sécuriser vos données.

Études de cas

Peut-être que tout ceci ne vous a pas encore permis de prendre une décision quant à vos besoins. Rappelez-vous qu'**IDCLIC** est à votre disposition pour vous conseiller. Pour vous aider un peu plus, nous vous proposons quelques cas de figure fréquents qui correspondent peut-être à votre situation.

1. Renouveler mon équipement

« Notre serveur est assez ancien, il montre quelques signes de faiblesse. J'hésite à le changer par un nouveau. On m'a dit que je devrais idéalement mettre de nouveaux disques durs dans ce nouveau serveur. Au vu de l'investissement minimum (environ 500 €), je me demande s'il ne serait pas pertinent de passer tout sur un hébergement Cloud. »

C'est une bonne idée de passer tout sur un *Cloud*. Certaines personnes sont un peu frileuses à l'idée de confier toutes leurs données à une société extérieure (qui plus est sur Internet). Nous en parlions au début de ce document, côté sécurité, ces sociétés sont obligées de « montrer patte blanche » quant à la confidentialité et la robustesse de leurs systèmes. Il n'est pas rare qu'elles implantent dans leurs systèmes un cryptage en 256 bits, ce qui est très robuste.

Cependant, vous préférez peut-être garder un accès « physique » à vos données. Dans ce cas, l'investissement dans un nouveau matériel est peut-être à considérer. Si vous êtes éligible pour un *Office 365 pour associations* gratuit, c'est une opportunité qu'il faut également prendre en considération.

2. J'ai déjà un équipement récent

« Nous avons acheté un serveur voici un an, nous l'avons équipé de disques durs de 2 To. Je n'ai donc besoin de rien… En plus de cela, je procède chaque semaine à un backup sur disque dur externe. »

Effectivement, vous avez un équipement (probablement) sûr, de bonne qualité. Vous procédez à des backups, c'est une excellente idée. Cependant, comme expliqué plus haut, si votre backup demeure au même endroit que votre serveur, en cas de sinistre dans votre bâtiment, votre disque dur pourrait être inutilisable tout autant que votre backup.

Nous vous recommandons de penser à un backup distant ou, au moins de procéder à un autre backup (sur un autre disque nomade à déplacer hors de vos murs). Gardez cependant à l'esprit que cette dernière possibilité peut au fil du temps altérer le disque externe qui souffrira des déplacements et des écritures répétées. Par contre, en utilisant un backup distant, l'opérateur se charge de maintenir un matériel en état en permanence.

3. Je n'ai rien, tout va bien…

« Serveur, backup, … On n'y a jamais vraiment pensé, on n'a jamais de problème. Ce sont des frais certainement inutiles et du travail supplémentaire pour procéder aux backups. »

C'est vrai, tout va bien et pourvu que ça dure ! Mais vous pouvez nous croire : il n'y a rien de pire que de perdre toutes vos données habituellement si accessibles. Tellement accessibles d'ailleurs qu'on ne se rend même plus compte de leur fragilité. Selon nous, il est très urgent dans ce cas de vous protéger contre la perte de vos données. Quant au prix, il est vrai que cela représente des frais supplémentaires. Mais combien pourrait vous coûter la perte de vos données ? Combien de temps faudra-t-il pour tout recréer (pour autant que vous puissiez tout recréer). Cela aussi représente un coût.

Quant au travail supplémentaire nécessaire pour procéder aux backups, les procédures automatisables peuvent être réalisées sans aide humaine récurrente.

4. Backup ou Cloud ?

« Comme nous n'avons rien, pas de serveur, pas de backup, pourquoi ne pas prendre un 'tout-en-cloud' ? »

Excellente idée ! Selon les avis, certaines personnes préfèreront tout de même avoir une copie des données physiquement présente sur site. C'est une question de choix mais aussi de budget, de calcul à court et à long terme.

5. Le travail à distance…

« L'épidémie de COVID nous a obligé à travailler à distance, ce qui nous a contraint à prendre des dispositions, notamment pour la disponibilité de nos fichiers. Comment éviter de faire des copies de fichiers sur des clés USB ou autres supports ? D'autant que nous risquons de dupliquer des fichiers et d'avoir des versions différentes ? »

Bien entendu, ce nouveau contexte nous pousse à reconsidérer notre point de vue sur la question. Une fois encore, plusieurs possibilités existent et un choix doit être fait. Selon les cas, il peut être intéressant de tout déplacer vers un *Cloud*. Il faut cependant garder à l'esprit qu'on ne peut pas migrer l'ensemble des fichiers vers cette solution en un simple clic ni en quelques secondes. Il faut également que personne ne travaille sur les fichiers durant le déplacement. Cela s'organise !

Comme déjà évoqué plus haut, ce choix peut être judicieux si l'opportunité se présente pour le remplacement d'un matériel obsolète. Dans ce cas, utiliser un système de type *Drive* permet aussi de gérer efficacement les problèmes d'utilisation concurrente de fichiers. Il faut cependant garder en tête que de tels systèmes génèrent habituellement des copies locales des fichiers. Dès lors, si vous disposez d'une grande quantité de fichiers sur votre *Drive* et qu'ils sont synchronisés sur votre ordinateur, vous consommerez beaucoup de place sur votre disque dur.

Par contre, si vous ne souhaitez pas migrer vos fichiers vers un tel système, il vous reste la possibilité d'utiliser un *VPN* (réseau privé virtuel) ou mieux, d'utiliser les réseaux définis par software (SD-LAN). Dans les deux cas, tout se passe comme si vous étiez physiquement sur votre lieu de travail alors que vous y êtes connecté à distance.

Si vous souhaitez utilisez pareilles solutions, contactez IDCLIC. Nous vous aiderons à faire le bon choix et pourrons vous assister pour sa mise en œuvre.

Conclusion

La sécurité des données est une affaire cruciale. Malheureusement, c'est une question qui n'est pas toujours au centre des préoccupations. Nous remettons souvent cela à plus tard, estimant que ce n'est pas vraiment une priorité. C'est souvent lorsqu'un pépin se produit et qu'il y a de lourdes conséquences que réalisons tout ce qui aurait pu être mis en place pour l'éviter.

Les événements sanitaires de 2020 nous ont également montré à quel point il est nécessaire de rester connecté à nos données. Les outils ne manquent pas mais il faut bien reconnaître qu'il n'est pas aisé de s'y retrouver.

Nous espérons que ces quelques informations vous ont permis d'y voir plus clair.

Nous sommes en mesure de vous conseiller mais aussi de vous aider à mettre en place la meilleure solution, parfaitement adaptée à votre environnement de travail, à vos besoins mais aussi à votre budget. Contactez-nous !

Pour nous contacter :

frederic.wauters@idclic.be - www.idclic.be