LIVRE BLANC

TPE : Comment protéger ses données

iakaa™

L'assistance informatique à distance

SOMMAIRE

Introduction :
Perte de données : comment éviter le drame.

La perte de données est la bête noire de tout possesseur d'ordinateur, et plus particulièrement des entrepreneurs et des TPE. Or, pour une entreprise, la perte de données peut être fatale. De plus, dans la plupart des cas cette perte est due à une erreur humaine. Iakaa vous donne quelques conseils pour protéger et conserver vos données avant qu' il ne soit trop tard.

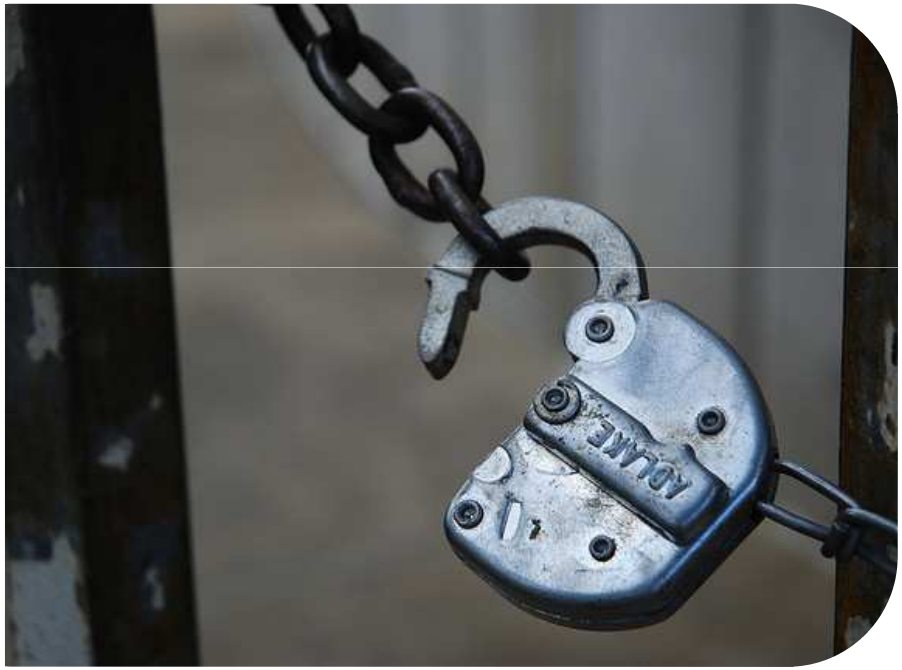
Sauvegardez en externe :
La méthode la plus sûre est encore de stocker vos documents, bases de données et autres fichiers importants sur un disque dur externe. Transférez vos fichiers régulièrement afin de conserver un double de vos documents majeurs en cas de perte totale de données.

Prenez soin de votre matériel :
Certains dégâts matériels physique de votre ordinateur peuvent rendre impossible la récupération des données qu'il contient. Soyez prudent et veillez à la bonne santé de votre équipement informatique. Si vous changez de matériel d'alimentation (batterie ou chargeur), choisissez un équipement conçu spécifiquement pour votre machine.

Ne jouez pas les héros :
En cas de disparition de vos données, ou de bug, ne présumez pas de vos compétences, ne tentez pas de résoudre le problème vous-même. Contactez un professionnel. En effet, le fait que vous ne puissiez pas accéder à vos fichiers ne signifie pas qu'ils aient complètement disparu. Un informaticien qualifié pourra peut-être les récupérer.

75% des réseaux Wifi ne sont pas sécurisés

Avast vient de révéler dans une récente étude que les réseaux wifi des Français sont, pour la plupart, mal protégés et vulnérables aux cyber-attaques. En effet, 75% des wifi français ne sont pas sécurisés. Ces failles ont dues pour 80% des cas à un problème de mot de passe trop simple. Il est donc facile d'y remédier.



Le réseau Wifi : une porte d'entrée sur vos données

10% des routeurs ne sont pas protégés par un mot de passe. 24% le sont par un mot de passe trop simple comme un nom, un prénom, une adresse ou une date, que les pirates peuvent aisément deviner. 50 % des réseaux sont protégés par **le mot de passe par défaut du constructeur** comme *admin* ou *1234* par exemple (une porte grande ouverte aux attaques informatiques). Pourtant via votre wifi, les pirates ont accès à votre ordinateur, mais aussi à vos périphériques, smartphones, tablettes ou objets connectés. Ces équipements recèlent de nombreuses informations capitales et il est important de les protéger. Les cyber-attaques menacent **votre sécurité, vos données et vos équipements informatiques.**

Malgré ces chiffres alarmants, **42%** des Français pensent que leur réseau est protégé. Ce qui montre une flagrante méconnaissance des bonnes pratiques en matière de sécurité. L'accès aux réseaux privés est très facile. Pour preuve, 5% des Français avouent utiliser frauduleusement le réseau de leur voisin. **20%** des Français ont déjà été piratés et 34% craignent le vol de leurs informations personnelles.

Les foyers français ne sont pas les seuls à être vulnérables au cyber-attaques via leur réseau wifi : en effet **les petites entreprises** sont elles aussi mal protégées et ce manque de confidentialité peut avoir de graves répercutions économiques en cas de **piratage**. Avast à annoncé qu'il lancera en janvier 2015 une gamme de solutions gratuite pour **la sécurité des données des TPE**.

Choisir un bon mot de passe pour sécuriser vos données

Le nom de votre entreprise, votre code postal, votre date de naissance constituent des choix de mots de passe potentiellement dangereux. Voici quelques conseils pour choisir le mot de passe idoine et mettre à l'abri vos données numériques.

« Password », « 12345 », « Monkey », « 0000 »… Voici quelques-uns des mots de passe les plus utilisés au monde. Avec des choix aussi communs, les équipements informatiques deviennent de véritables passoires, ouvertes aux attaques en tout genre. Il existe pourtant quelques mesures élémentaires à respecter pour choisir un mot de passe efficace.

Créer des mots de passe sécurisés :

Des mots de passe correctement sécurisés sont indispensables à la sécurité de vos données professionnelles. Mais quelles sont les caractéristiques d'un mot de passe sûr ? Voici comment choisir le mot de passe parfait.
Tout d'abord, oubliez les dates de naissance, noms de famille et autres « azerty123 » ils figurent en premier sur la liste des mots testés par les pirates pour accéder à vos comptes. Un bon mot de passe doit comporter au minimum
 :
- 12 caractères
- des lettres mais aussi des chiffres
- des majuscules
- des caractères spéciaux si possible

Si vous manquez d'inspiration, le web regorge de générateurs de mots de passe. Il suffit d'entrer le nombre et le type de caractères souhaités, et le générateur crée un mot de passe de manière aléatoire.

D'autre part, n'utilisez pas un seul et même mot de passe pour tous vos sites, outils ou boîtes mail. En effet, l'effraction d'un seul de vos compte donnerais accès à l'ensemble de vos accès sécurisés. Choisissez un mot de passe unique pour chacune de vos souscriptions. Si l'effort de mémoire vous parait trop difficile, nous vous conseillons d'utiliser au moins 3 mots de passe différents en fonction des types de compte.
Enfin, pour plus de sûreté, pensez à changer tous vos mots de passe chaque année.

Le nombre de caractères

Pour une sécurité maximale, privilégiez un mot de passe à plus de dix caractères. Selon le portail officiel de la sécurité informatique en France, un robot spécialisé mettrait environ une heure pour craquer un mot de passe de huit caractères alors qu'il lui faudrait un mois pour un mot de passe qui en comporte dix. Mieux vaut donc éviter de faire court.

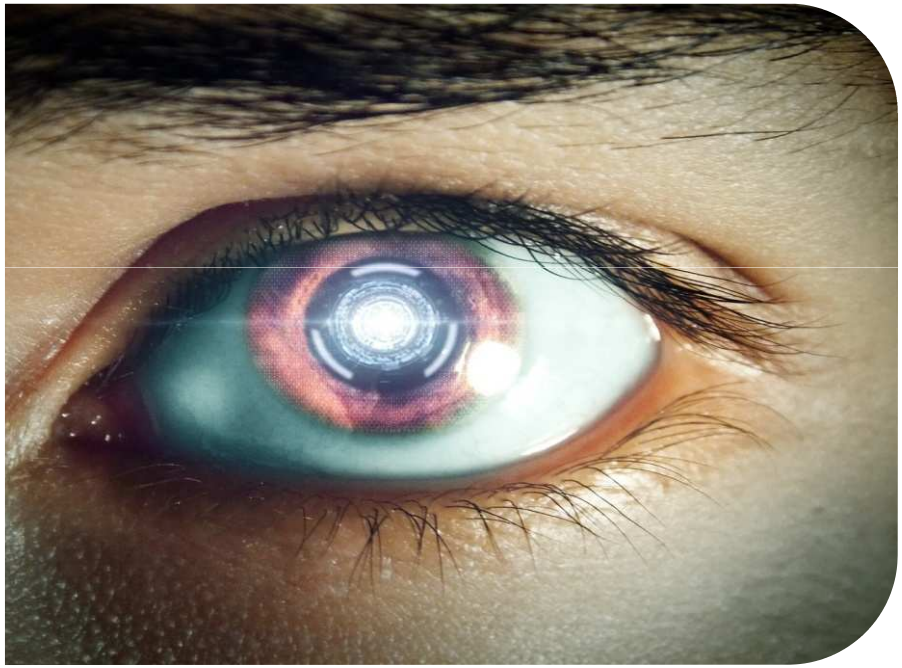
Le type de caractères

Un mélange de caractères numériques et de caractères alphabétiques permet une meilleure sécurité du mot de passe. Cette sécurité est d'autant plus renforcée si vous mélangez des lettres capitales et des lettres minuscules.
Ces deux critères peuvent très vite donner des mots de passes extrêmement compliqués et difficiles à retenir. Utilisez alors des moyens mnémotechniques pour choisir et retenir ces mots de passe complexes.

La diversification des mots de passe

Nous avons tendance à adopter un seul et unique mot de passe pour différentes utilisations (PC, réseaux sociaux, e-mails, etc.). Or, cette pratique comporte des risques. Un mot de passe n'est efficace que s'il couvre un domaine ou un nombre d'équipements restreint. Ainsi, mieux vaut diversifier ses mots de passe pour contrer au mieux les risques.

La biométrie va-t-elle supplanter le mot de passe ?



A priori, le mot de passe serait un système de sécurité faillible, susceptible d'être aisément piraté. Rien n'est plus faux. Le mot de passe constitue une protection fiable, ses failles proviennent de la manière dont nous l'utilisons. Les utilisateurs ne retiennent pas les mots de passe sûrs mais complexes et leur préfèrent des mots de passe plus simplistes et donc plus vulnérables. De plus, dans l'univers professionnel, les mots de passe sont souvent partagés avec les collègues. Tous ces usages affaiblissent la sécurité potentielle des mots de passe. Il s'agit donc de trouver un nouveau moyen de sécuriser l'accès à nos espaces privés. La biométrie apparaît comme une procédure simple et sécurisée d'identification qui pourrait bien remplacer l'usage des mots de passe.

Les failles de la biométrie :

En réalité, chaque méthode montre **des avantages et des failles**. Il peut être facile de leurrer un système biométrique. Et si un mot de passe piraté peut être changé, ce n'est pas le cas pour une **empreinte digitale**.
D'autre part, en entreprise, la **technologie biométrique** semble difficile à mettre en place car coûteuse. De plus, les sociétés particulièrement soucieuses de leur sécurité sont méfiantes à l'égard des **innovations technologiques** et attendent qu'un système soit éprouvé pour l'adopter. Ce qui laisse au mot de passe de beaux jours devant lui.

Des systèmes de sécurités complémentaires :

Aucun système de sécurité n'est fiable à 100% et la biométrie n'a pas vocation à être utilisée comme seul rempart. Cette technologie doit être associée à l'emploi d'un mot de passe. Multiplier les barrières de sécurité est le moyen le plus sûr de **protéger ses données**. Mais attention, doubler les facteurs d'identification ne doit pas être une excuse pour **négliger la complexité d'un mot de passe**. Tout système présente **des vulnérabilités** et la principale faille du mot de passe réside dans sa **mauvaise utilisation**. Il faut avant tout changer **les comportements des usagers**. La biométrie présente l'avantage de réduire les risques liés à une erreur humaine.
Ainsi, ne nous inquiétons pas pour l'avenir du mot de passe. La biométrie n'est pas sa concurrente mais bien son **complément**. Et en attendant la généralisation des systèmes de sécurité biométriques, assurez-vous de choisir des mots de passe **diversifiés et efficaces**.

Les TPE : cibles privilégiées des hackers

Les annonces d'intrusion informatique dans les grandes entreprises se multiplient. Mais les TPE-ne sont pas épargnées pour autant, bien au contraire. Les attaques informatiques contre les entreprises de moins de 250 salariés ne cessent d'augmenter.

Les TPE sont des cibles particulièrement vulnérables et donc privilégiées pour les pirates informatiques. En 2012, 31% des cyberattaques visaient une PME contre 18% en 2011 et cette tendance ne cesse de se confirmer. En effet les données des TPE : données commerciales ou propriété intellectuelle, permettent d'atteindre les grandes entreprises avec qui les TPE travaillent. Pourtant les petites entreprises s'estiment toujours plus à l'abri des attaques informatiques que les grands groupes.

Des méthodes de plus en plus sophistiquées :

Les hackers exploitent des failles dans le système informatique des TPE. Elles peuvent être classées en deux catégories : les failles techniques et les failles humaines. Les failles techniques sont la conséquence d'une protection informatique quasi voire totalement inexistante dans l'entreprise : une connexion Wi-Fi non sécurisée ou un réseau directement connecté à Internet par exemple. Mais les failles techniques seraient beaucoup plus difficiles à exploiter sans les failles humaines de l'entreprise. En effet, les nouvelles techniques comme le phishing (technique qui consiste à se faire passer pour un tiers de confiance afin d'inciter à divulguer des informations confidentielles) ou encore le watering hole (l'insertion d'un virus sur un site web fréquemment visité par la cible) exploitent la négligence des employés pour s'attaquer aux données de l'entreprise.

Mieux vaut prévenir que guérir :

Par manque de moyen mais aussi d'informations vis-à-vis des attaques informatiques, les TPE négligent leur sécurité informatique. Il est alors très facile pour des hackers de pénétrer leur système d'information et de capturer leurs données. Les conséquences d'une attaque informatique coûtent de plus en plus cher, cela peut se compter en millions d'euros. Bien moins cher, l'investissement dans un système de sécurité informatique vous permettra de vous protéger contre un piratage informatique. Cette protection doit être combinée avec de la prévention auprès de vos employés sur tous vos canaux de communication (e-mailing, téléphone,…).

Enfin si malgré cela vous êtes victime d'une attaque informatique, portez plainte immédiatement auprès de la BEFTI (Brigades d'Enquête sur les Fraudes aux Technologies de l'Information). Pour cela il vous faudra fournir plusieurs éléments dont l'adresse exacte de la ou des machine(s) attaquée(s), la liste de tous les préjudices engendrés par l'attaque et une trace informatique de l'intrusion. Pensez donc à effectuer une sauvegarde des logs sur les applications impactées, les systèmes d'exploitation et les systèmes de sécurité ainsi qu'une copie physique (sur un disque dur externe) du disque dur dans son état au moment de l'intrusion.

TPE : Comment sauvegarder ses données

La sauvegarde de données est un élément stratégique pour une entreprise quel que soit sa taille. Conscientes du risque encouru en cas de perte de leurs données, les TPE sont pourtant peu nombreuses à mettre en place un dispositif adapté.
Une récente étude publiée par Paragon Software, fournisseur mondial de solutions de stockage et de protection de données, a révélé les habitudes des TPE en matière de sauvegarde de données. 22% ont déclaré avoir perdu des informations stratégiques pour leur activité avant d'avoir eu recours à une solution de sauvegarde. Les causes d'une perte de données sont diverses : vol, sinistre, défaillance informatique, piratage… Le recours à un dispositif de sauvegarde est donc essentiel, d'autant plus lorsqu'on sait que 80% des entreprises ayant connu une perte importante de leurs données disparaît dans les deux ans qui suivent (Source SNIA France).

Les différentes méthodes de sauvegarde

La méthode de sauvegarde la plus simple pour les données de votre entreprise est la sauvegarde complète, elle consiste à réaliser une copie conforme de l'ensemble de vos données sans distinction. Cette méthode particulièrement fiable peut néanmoins poser des problèmes de lenteur en fonction du volume de données à sauvegarder et être coûteuse en termes d'espace disque. Deux autres méthodes permettent de contourner ces inconvénients: la sauvegarde incrémentale et la sauvegarde différentielle. La sauvegarde incrémentale ne copiera que les fichiers qui ont été modifiées depuis la sauvegarde précédente. La sauvegarde différentielle quant à elle se focalisera sur tous les fichiers qui ont été modifiés depuis la dernière sauvegarde complète.

Parmi les solutions de sauvegarde de données, plusieurs options s'offrent aux TPE. Si votre entreprise compte peu de postes informatiques, les sauvegardes de données peuvent s'effectuer directement sur vos ordinateurs, avec une seconde sauvegarde en parallèle sur un support mobile (clé USB, DVD ou disque dur externe). Si vous possédez plus de 5 postes informatiques, la sauvegarde sur un serveur dédié à l'entreprise limite considérablement les pertes de données puisqu'elle s'effectue automatiquement et quotidiennement. Enfin la sauvegarde par Internet ou télé-sauvegarde consiste à connecter les ordinateurs de l'entreprise à un serveur distant, placé chez un prestataire informatique qui effectue lui-même la sauvegarde de vos données. Peu coûteuse et fiable, cette dernière solution est de plus en plus plébiscitée par les professionnels.

Le Cloud : une solution adaptée aux professionnels

Un utilisateur professionnel sur dix. C'est la proportion qu'a pris la bureautique Cloud ou « dans les nuages » chez les pros. Cette proportion va augmenter rapidement dans les prochaines années.
Avec 50 millions d'utilisateurs professionnels à travers le monde, la bureautique « dans le Cloud » ne s'est pas encore généralisée dans les entreprises. Pourtant, le *Cloud Computing*, cette manière de fournir des solutions informatiques en ligne ne date pas d'hier. L'un des premiers sites Web de services de *Cloud Computing* n'est autre que Google, lancé en 1999. Et pourtant, l'informatique dans les nuages commençait déjà à germer dans les années 60…

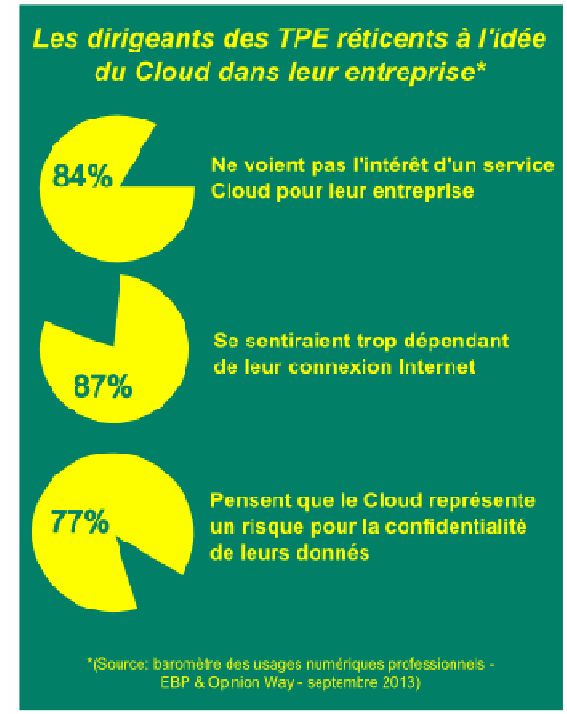
Seuls 8 % des professionnels sont « dans les nuages »

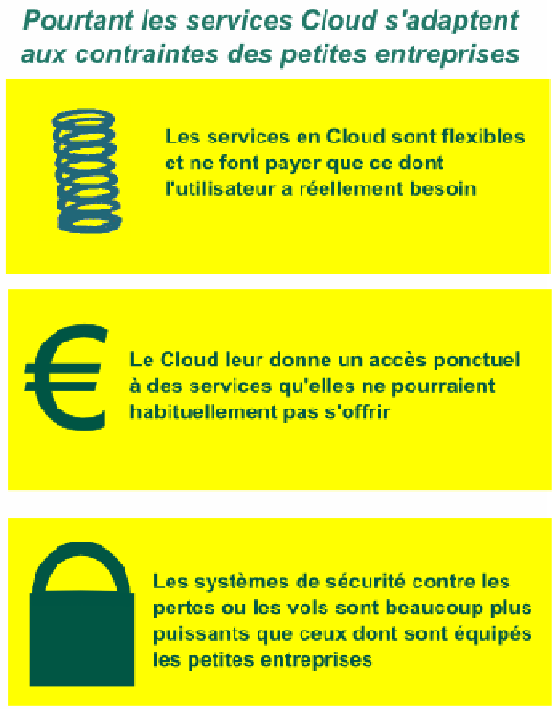
Le *Cloud Computing* offre de nombreux avantages aux professionnels notamment au niveau économique : les solutions techniques étant délocalisées (maintenance, service informatique, serveurs etc.), leur coût devient fixe. Pourtant, selon une étude du cabinet de conseil Gartner, le *Cloud Computing* n'est utilisé que par 8 % des entreprises dans le monde (hors Chine et Inde). Pourquoi ce faible taux d'adoption ? Parce que les entreprises hésitent bien souvent à confier des données confidentielles à un prestataire extérieur, généralement basé à l'étranger. Et ce n'est pas l'affaire PRISM (système d'espionnage en ligne américain) qui va les rassurer !

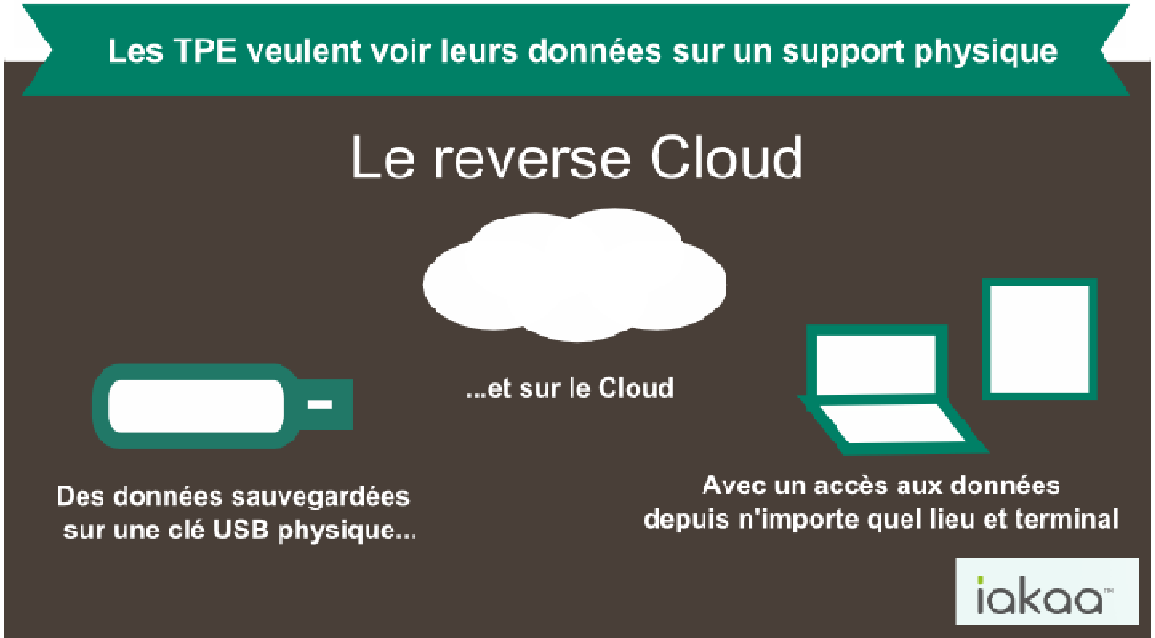
Multiplication des terminaux : un facteur d'évolution

Mais cette tendance pourrait rapidement s'inverser. Toujours selon la même étude, la proportion des utilisateurs du *Cloud Computing* pourrait représenter 50 % des professionnels d'ici les dix prochaines années. Un phénomène soutenu par la multiplication des terminaux d'accès à Internet. Si en 2007, seul le PC était utilisé pour se connecter à un espace de travail en ligne, aujourd'hui les tablettes, Smartphones et autres PC portables sont autant de nouveaux terminaux utilisés dans le cadre professionnel. Dans ce contexte, les solutions SaaS deviennent bien plus économiques et offrent plus de flexibilité, notamment pour les TPE.

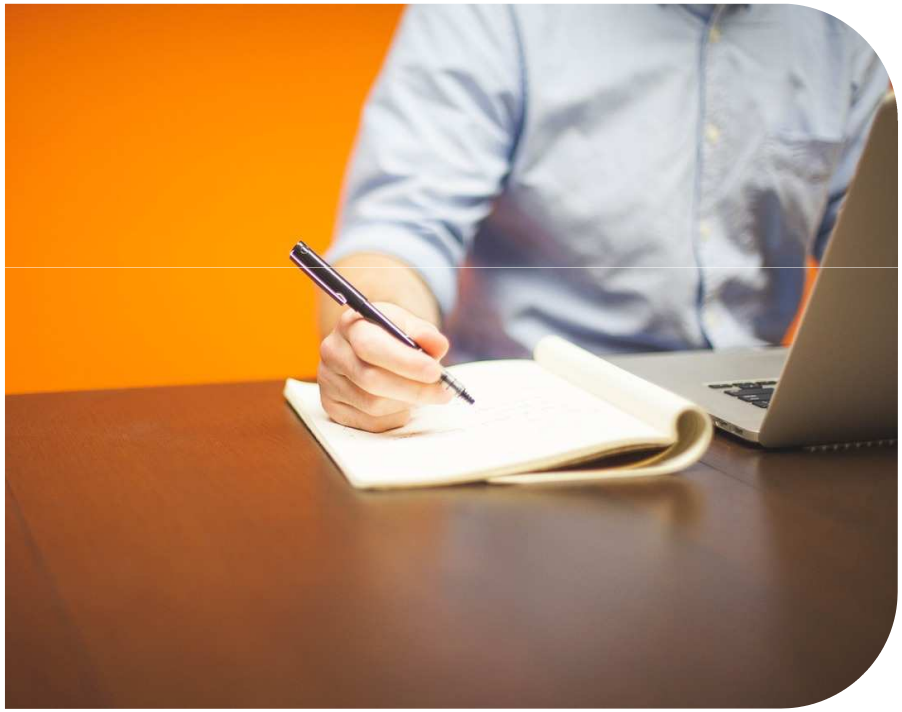
Le Cloud: une solution hybride pour les TPE







Sécurité : Qu'est-ce qu'un PRA ?



Votre système informatique a subi un sinistre ? Un Plan de Reprise d'Activité ou PRA permet à votre entreprise de reconstruire son infrastructure. Les principales questions à se poser pour le mettre en place.

Incendies, inondations, cambriolages, attaques informatiques… ça n'arrive qu'aux autres ! Beaucoup de chefs d'entreprise pensent que la probabilité de subir de tels sinistres est faible. Pour eux, il est donc inutile de consacrer du temps à élaborer un plan d'action pour y faire face. Pourtant, cette impréparation peut s'avérer fatale à leur entreprise. Par exemple, en ce qui concerne le piratage, 71% des TPE ne s'en remettent pas. Pour éviter la catastrophe, le *Disaster Recovery Plan* ou Plan de Reprise d'activité est un outil efficace. Voici les cinq questions clés à se poser pour élaborer votre PRA.

Quels sont les différents scénarios-catastrophe possibles ?

Première étape de votre plan de reprise d'activité : lister toutes les catastrophes envisageables y compris les plus improbables. Bien sûr, il faut rester réaliste. N'anticipez pas un raz-de-marée qui puisse toucher Paris. En revanche, une destruction de l'intégralité de vos données suite à une cyberattaque particulièrement puissante est un scénario possible.

Quel est le rôle de chacun en cas de problème ?

Le meilleur moyen pour éviter la panique lors d'une catastrophe est d'anticiper les rôles de chacun. Cela passe par la sensibilisation de vos collaborateurs au risque, leur formation à la gestion de crise et la définition d'un périmètre de responsabilité. Ainsi, l'entreprise pourra se mettre très rapidement en ordre de bataille en cas de problème informatique majeur.

Quelles sont les applications critiques pour l'entreprise ?

Afin de bien anticiper les risques, chaque module applicatif de votre entreprise doit être évalué afin d'établir son niveau d'importance dans votre système informatique. Ainsi, vous pourrez estimer et budgéter les besoins de sauvegarde et de restauration pour vos données stratégiques.

Comment évaluer la fiabilité de son PRA ?

Comme les exercices de sécurité-incendie, les PRA doivent être répétés de façon régulière afin de tester leur efficacité et la maîtrise du rôle de chacun.

Faut-il faire évoluer son PRA ?

L'informatique évolue très vite et votre Plan de Reprise d'Activité doit s'y adapter. Un renouvellement régulier du PRA est donc indispensable afin que votre entreprise soit toujours prête face aux imprévus.

Conclusion : Les bonnes pratiques de sécurité pour les TPE

L’application de tous ces points impose de définir une véritable politique de sécurité informatique dans et hors de l’entreprise. Recensez les applications et pratiques que vous souhaitez autoriser et celles que vous voulez interdire. Formez vos collaborateurs aux bonnes pratiques (choix de mots de passes, repérage des applications dangereuse…). Rendez cette politique officielle en la publiant dans le règlement interne de l’entreprise ou en la faisant signer par vos collaborateurs. N’oubliez pas de renouveler les termes de votre politique régulièrement en fonction des évolutions et des changements de votre matériel.

Entretenez votre réseau

Pour des performances optimales, rien de tel qu'un entretien régulier ! Cela passe principalement par la vérification des mises à jour des logiciels mais aussi par la désinstallation des logiciels obsolètes ou inutiles à votre activité. Même si la plupart des mises à jour peuvent se faire automatiquement, une vérification régulière est toujours utile.

Fragmentez votre réseau

Une sécurité optimale passe par un découpage de votre réseau en différentes zones. Une zone peut être réservée aux collaborateurs de l'entreprise avec une sécurité renforcée. Une autre zone peut être réservée aux clients et prestataires extérieurs avec un accès Internet sans que ceux-ci puissent accéder au réseau interne de l'entreprise. Autre segmentation possible : le découpage par service (financier, marketing, commercial…).

Distribuez les droits d'administration avec parcimonie

Vos terminaux informatiques sont accessibles via des comptes utilisateur et des comptes administrateurs. Ces derniers sont sensibles et stratégiques car ils donnent un accès très large aux données de votre entreprise. D'où l'intérêt de limiter l'accès à ce genre de compte aux seuls collaborateurs qui en auront vraiment l'usage, comme par exemple le responsable informatique ou un membre du comité de direction.

Faites appel à des experts.

iakaa™

L'assistance informatique à distance

Le téléassistance est un moyen efficace pour renforcer la sécurité informatique dans votre entreprise, notamment l'élimination de virus, l'optimisation de votre ordinateur, l'installation de logiciels, les nettoyages, mises à jour, paramétrages ou tout problème de sécurité informatique… En effet, beaucoup d'incidents sont dus à de mauvaises configurations ou à la présence de virus informatiques et ne nécessitent pas d'intervention physique sur l'ordinateur. Pour ce type de cas, le télédépannage est la solution optimale.

Iakaa vous accompagne :

La procédure est simple et assure une aide efficace et rapide. Il suffit que votre ordinateur soit connecté à internet. L'entreprise est joignable par téléphone pour répondre à toutes vos questions. D'autre part, iakaa ne propose pas d'abonnement, vous ne payez que lorsque vous en avez besoin et si votre problème est résolu. Un service accessible, à l'écoute quel que soit la raison de votre appel ou votre niveau de compétence en informatique. iakaa est toujours à vos côtés pour trouver avec vous la solution à toutes vos déconvenues.

En bref iakaa c'est

Une solution fiable et sécurisée
Un service qui s'adapte à vos besoins
Un dépannage rapide et efficace
Une façon simple de résoudre vos problèmes informatiques sans vous déplacer.

Contactez-nous :

www.iakaa.com
09.73.87.25.20
http://blog.iakaa.com/
Ou sur nos comptes Facebook
et Twitter @IakaaTeam