# Guides de sécurité pour les petites entreprises

Sécurisation de votre start-up ou de votre petite entreprise

AVG AU TRAVAIL

# Maintenir les systèmes en fonctionnement et sécuriser les informations dans un monde en ligne

Les petites entreprises peuvent subir des heures d'interruption de leur activité chaque année sur chaque ordinateur utilisé en interne, tandis qu'au cours des deux dernières années, le vol d'identité et d'informations est devenu la préoccupation de sécurité majeure des chefs d'entreprise.

« Une brèche de la sécurité est beaucoup plus susceptible d'entraîner des conséquences catastrophiques sur le chiffre d'affaires ou même sur la survie d'une start-up ou d'une petite entreprise. »

Le paysage technologique dans les petites entreprises et les ressources dont elles disposent pour repousser les logiciels malveillants sur Internet sont généralement bien différents de ceux qui existent dans les grandes entreprises. Pourtant, une brèche de la sécurité est beaucoup plus susceptible d'entrainer des conséquences dramatiques pour leur chiffre d'affaires ou même sur la survie d'une start-up ou d'une petite entreprise.

Ce guide présente quelques étapes simples, mais efficaces, que vous pouvez suivre pour assurer la sécurité de vos actifs professionnels précieux et des données de vos clients. Utilisez les conseils présentés à la fois lorsque vous créez votre entreprise et par la suite, à titre de référence, tous les trois mois environ, pour vous assurer que vous respectez les bonnes pratiques et faites tout le nécessaire pour assurer la sécurité de votre entreprise et de vos employés en ligne.

# Les bases de l'entreprise :

# Trois étapes essentielles pour protéger votre activité

La sécurisation de votre entreprise contre les logiciels malveillants sur Internet est une opération relativement simple, mais qui nécessite une certaine réflexion et un petit investissement en argent et en temps. Toutefois, si vous prenez ces mesures dès maintenant, le temps et le coût nécessaires seront largement moindres que ceux qu'occasionnerait la perte de revenu et de temps de gestion nécessaire pour faire face aux problèmes de sécurité qui sont susceptibles de se poser ultérieurement si vous n'êtes pas correctement sécurisé

Lorsque vous pensez à la sécurité en ligne de votre entreprise, n'oubliez pas le fameux adage médical : mieux vaut prévenir que guérir.

Les étapes essentielles à suivre peuvent se diviser en trois catégories : stratégie, technologie et processus.

### Stratégie

1. Décidez si les ordinateurs de bureau et portables et les logiciels doivent être fournis par votre entreprise ou par vos employés, et tenez compte de ces décisions dans vos stratégies, vos achats et vos processus.

2. Mettez en place une stratégie simple d'utilisation acceptable pour tout ordinateur utilisé dans l'entreprise et pour tout support servant à stocker ou à transporter des données de l'entreprise.

3. Créez une stratégie de solidité acceptable des mots de passe et assurez-vous que tous les ordinateurs et autres équipements informatiques sont protégés par des mots de passe.

4. Exigez que tous les incidents de sécurité soient rapidement signalés à un responsable de l'entreprise et gérés.

### Technologie

1. Veillez à ce que tous les systèmes d'exploitation et les applications soient mis à jour à l'aide des derniers correctifs de sécurité à mesure qu'ils sont commercialisés - en utilisant de préférence une technologie de mise à jour automatique.

2. Assurez-vous que tous vos ordinateurs sont équipés d'une suite logicielle de sécurité.

3. Chaque ordinateur devrait disposer de son propre pare-feu, en plus du pare-feu éventuellement installé au niveau de l'entreprise.

4. Si vous gérez vous-même vos serveurs de stockage de fichiers et de messagerie, assurez-vous qu'ils sont également dotés d'un logiciel de sécurité à jour

### Processus

1. Veillez à ce que tout le personnel reçoive une formation de base à la sécurité en ligne et des instructions via vos stratégies

2. Assurez-vous que tous les fichiers, données, messages et autres systèmes de l'entreprise sont régulièrement sauvegardés

3. Modifiez régulièrement tous les mots de passe, notamment lorsqu'un employé ou un sous-traitant quitte l'entreprise. Remplacez en particulier les mots de passe d'administrateur ou les mots de passe partagés sur des réseaux ou des systèmes centralisés

4. Prenez au sérieux les brèches de sécurité : isolez tout système compromis du reste du réseau et faites appel le cas échéant à un professionnel de la sécurité informatique pour qu'il vérifie que le logiciel malveillant est bien éliminé

# Stratégie de sécurité informatique

## Cette section fournit des détails plus précis sur les éléments clés d'une stratégie de sécurité informatique dans les petites entreprises

En tant que petite entreprise, vous ne vous souciez sans doute pas exagérément de stratégies documentées et précises. Pourtant, la plupart des petites structures disposent au moins d'un « Manuel destiné au personnel », regroupant les règles à respecter dans l'entreprise et qui vient compléter les lettres d'embauche et les contrats, ne serait-ce que pour éviter les poursuites devant le Conseil des Prudhommes !

Le Manuel destiné au personnel peut également décrire vos principales stratégies en matière d'utilisation des équipements informatiques et des données de l'entreprise et la plupart des modèles de manuels de ce type que vous pouvez télécharger sur Internet ou obtenir auprès d'un avocat évoquent des dispositions de base dans ce domaine.

« Le manuel destiné au personnel est également l'endroit idéal pour décrire les principales stratégies de l'entreprise en matière d'utilisation de l'équipement informatique et des données de l'entreprise. »

Vous devriez cependant vous assurer que les dispositions du modèle dans la section sécurité informatique répondent à vos besoins et à ce titre, il est utile de tenir compte des éléments suivants :

**Matériel de l'entreprise ou matériel personnel**

Allez-vous fournir à vos employés et à vos sous-traitants tous les PC et ordinateurs portables qu'ils utiliseront ?

Bon nombre de grandes entreprises n'autorisent pas leur personnel à utiliser des ordinateurs personnels sur les réseaux de l'entreprise ou à des fins professionnelles. Toutefois, en tant que petite organisation, cette solution pourrait ne pas être pratique pour vous, surtout si vous faites fréquemment appel à des sous-traitants.

Si vous pouvez fournir tout l'équipement informatique, vous êtes également en position de choisir et d'installer les logiciels que vous autoriserez sur cet équipement.

En revanche, si vous avez l'intention d'autoriser des membres permanents ou temporaires du personnel à utiliser leurs propres ordinateurs, vous devrez décider si vous leur fournirez ou non des logiciels ou si vous leur demanderez d'utiliser les leurs.

Si les employés doivent utiliser leurs propres logiciels, vous devriez établir une liste des logiciels acceptables à utiliser dans le cadre de l'entreprise et inviter ces employés à exécuter une suite logicielle de sécurité et à maintenir leurs logiciels à jour - comme vous le feriez sur les ordinateurs appartenant à votre entreprise. N'oubliez pas que les équipements appartenant aux employés seront connectés à vos réseaux sécurisés et partageront les fichiers sensibles et les informations de votre entreprise avec les autres collaborateurs, les fournisseurs et les clients.

Sachez également que si les employés utilisent des logiciels qui ne disposent pas d'une licence adéquate, le fournisseur des logiciels peut avoir des droits sur les éventuels actifs générés grâce à ces logiciels : assurez-vous donc que votre stratégie interdit aux employés d'utiliser et d'installer des logiciels piratés ou sans licence.

Si vous avez l'intention de fournir les logiciels à utiliser sur les ordinateurs de l'entreprise, vérifiez que votre stratégie stipule que vous superviserez leur désinstallation chaque fois qu'un employé quittera l'entreprise.

# Mise en place d'une stratégie de sécurité

Cette section fournit des informations plus détaillées à propos de l'exécution d'une stratégie de sécurité informatique efficace

**Utilisation acceptable**

Il s'agit ici avant tout de décider si les employés pourront utiliser l'équipement et les logiciels de l'entreprise à des fins personnelles.

La plupart des entreprises acceptent cette utilisation personnelle, car il serait très compliqué et franchement, très démotivant de l'interdire.

Vous devriez cependant disposer au moins d'une stratégie interdisant l'installation de logiciels non requis dans le cadre de l'entreprise et naturellement, interdire l'affichage ou la rédaction de contenu susceptible d'offenser autrui. N'oubliez pas que la grande majorité des virus et logiciels espions sur Internet se dissimulent dans des documents, des images et des vidéos, conçus pour que les utilisateurs aient envie de les ouvrir.

Assurez-vous également que vous définissez des règles relatives au stockage des fichiers et des informations de l'entreprise sur des supports amovibles, tels que des clés USB, des disques durs externes et des CD/DVD inscriptibles. Il arrive trop fréquemment que les actifs d'une entreprise soient perdus ou divulgués en raison d'une négligence concernant ce type de périphériques ou parce que les informations qu'ils contiennent ne sont ni cryptées ni protégées par mot de passe.

**Stratégie de mot de passe**

Les mots de passe brefs, ou ceux qui ne comprennent qu'un ou deux mots, sont faciles à fracturer – voire à deviner – par les pirates, qu'ils soient humains ou automatisés.

Un bon mot de passe de « longueur minimum » doit comporter au moins 8 caractères et associer des lettres, des chiffres et éventuellement un autre caractère, tel qu'une apostrophe, un point d'exclamation ou un symbole dollar..

Les mots de passe permettant à l'administrateur d'accéder à l'équipement devraient comporter au moins douze caractères et sembler pratiquement aléatoires.

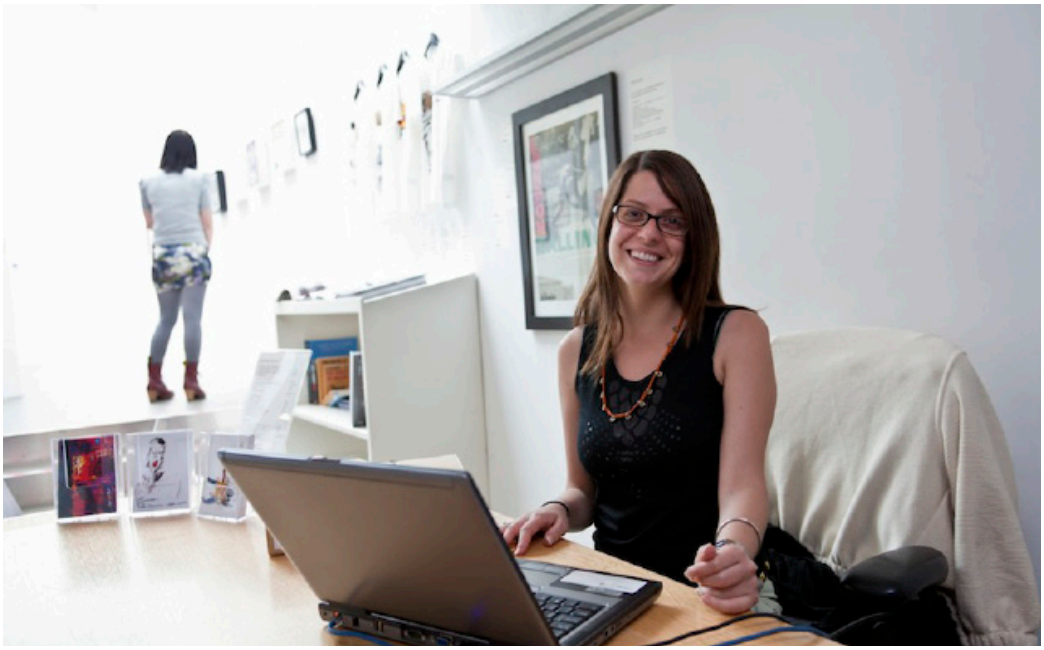
Enfin, assurez-vous que votre stratégie de mots de passe considère comme une infraction le fait de communiquer les mots de passe à toute autre personne, à l'intérieur ou à l'extérieur de l'entreprise, et de fournir des mots de passe partagés/d'administration à toute personne non agréée par les administrateurs de l'entreprise.

**Signalement des brèches**

Il peut arriver à tout le monde de recevoir un virus informatique ou de perdre des données de son entreprise de temps à autre. Pourtant, les employés hésitent souvent à signaler ces incidents, alors que leur silence ne fait qu'aggraver les choses, laissant le logiciel malveillant se propager ou la perte de données devenir publique et constituer une menace pour la réputation ou la propriété intellectuelle de l'entreprise.

Faites preuve d'indulgence avec les employés responsables d'une brèche de sécurité involontaire, à condition qu'ils aient respecté vos stratégies, mais précisez que le fait de ne pas signaler un incident constitue une infraction contractuelle sérieuse.

Il est indispensable d'être informé immédiatement de toute attaque de sécurité ou perte de données et de prendre les mesures techniques et de relations publiques appropriées pour gérer la situation.



« Il s'agit ici avant tout de décider si les employés pourront utiliser l'équipement et les logiciels de l'entreprise à des fins personnelles »

# Technologie des logiciels de sécurité

Cette section présente un aperçu des mesures techniques que vous pouvez prendre pour garantir la sécurité de votre entreprise sur Internet

Chacun sait qu'il doit installer un logiciel antivirus sur son ordinateur, même si malheureusement, la technologie antivirus à elle seule ne permet pas de mettre en place des barrières de protection entre votre équipement et vos fichiers et les logiciels malveillants qui rôdent aujourd'hui sur Internet.

Les logiciels gratuits ou en open source qui peuvent convenir aux particuliers ne sont généralement pas suffisamment complets pour la plupart des besoins professionnels, alors que les produits utilisés par les grandes entreprises requièrent souvent une infrastructure technique et des compétences en assistance informatique qui ne sont pas disponibles dans les petites sociétés : vous devez donc réfléchir soigneusement à vos besoins et à la gamme de logiciels de sécurité adaptée à votre entreprise.

**Mises à jour du système d'exploitation et des applications**

Les logiciels malveillants disposent de deux voies réelles pour s'exécuter sur l'ordinateur d'un utilisateur : soit en trompant l'utilisateur et en l'incitant à les exécuter manuellement, généralement en se faisant passer pour un élément amical ou une invitation, soit en s'exécutant automatiquement grâce à l'exploitation de lacunes des logiciels ou de « bugs » du système d'exploitation, du navigateur Internet, du logiciel de messagerie ou d'autres applications installées sur le PC.

Les fournisseurs commerciaux de systèmes d'exploitation et d'applications dépensent des sommes considérables pour identifier les nouvelles lacunes détectées dans leurs logiciels dès que les pirates et les criminels les trouvent et les exploitent, puis pour réparer rapidement ou « combler » ces lacunes.

Il est par conséquent extrêmement important de tenir à jour tous les ordinateurs de votre entreprise appliquant les derniers packs et correctifs. De plus, si vous ne disposez pas d'une équipe informatique qui se tient informée des nouveaux correctifs publiés et applique ces mises à jour, vous devez veiller à automatiser ce processus.

La plupart des logiciels commerciaux possèdent une fonctionnalité de mise à jour automatique qui devrait être activée. Sachez cependant que très souvent, ce n'est pas le cas des logiciels en open source, car les mises à jour ne peuvent pas franchir les processus rigoureux utilisés par les fournisseurs commerciaux pour garantir la compatibilité entre les logiciels.

Par conséquent, si vous avez l'intention d'utiliser sur le PC ou les serveurs de votre entreprise des systèmes d'exploitation ou des logiciels en open source, chargez au moins un employé de surveiller les mises à jour des logiciels, de les tester pour vérifier leur compatibilité lorsqu'elles sont publiées, puis d'inviter tous les autres employés à les installer.

« Les logiciels gratuits ou en open source qui peuvent convenir à certains utilisateurs ne sont généralement pas suffisamment complets pour répondre aux besoins des professionnels ».

## Logiciels de sécurité du serveur

Si vous utilisez des services de stockage, de messagerie ou d'intranet hébergés ou « en cloud » (dématérialisé), la sécurité de votre serveur doit être prise en charge.

Toutefois, si vous possédez vos propres serveurs, il est indispensable d'exécuter les logiciels de sécurité conçus pour les systèmes d'exploitation et les logiciels de messagerie que vous utilisez.

Si certains ordinateurs de votre réseau sont exposés à des logiciels malveillants, il est probable que la première chose que feront ces logiciels sera de tenter de se répliquer eux-mêmes sur tous les serveurs de fichiers qu'ils détecteront. Cependant, un bon produit de sécurité pour serveur de messagerie assure une protection contre les virus, le spam et les attaques par hameçonnage avant que les messages ne parviennent dans la boîte de réception de l'utilisateur où ce dernier pourrait les ouvrir.

Naturellement, vous devez aussi à vos fournisseurs et clients (moralement, si ce n'est légalement) de veiller à ce que tout e-mail que vous leur adressez par le biais de vos serveurs soit libre de tout logiciel malveillant. Or, un serveur de messagerie contaminé peut même être utilisé par les cybercriminels du monde entier pour distribuer leurs produits.

# Logiciels de sécurité en ligne

Un progiciel de sécurité complet vous protégera contre les virus, logiciels espions, attaques par hameçonnage (liens vers les sites Web qui vous orientent vers des sites différents) et assurera la détection et la prévention des activités que pourraient réaliser certains logiciels apparemment légitimes sur votre ordinateur, en analysant et en détectant le comportement aberrant des logiciels qui peuvent avoir été contaminés.

Pensez aux méthodes de détection présentes dans les logiciels que vous utilisez. Vous souhaitez que les logiciels malveillants soient détectés dès qu'ils arrivent dans les logiciels de messagerie de votre entreprise, votre messagerie instantanée ou via un téléchargement par un navigateur Internet... il ne faut pas risquer de voir ces logiciels être ouverts ou même exécutés.

Si votre entreprise opère principalement depuis un site unique, envisagez des fonctionnalités d'administration distantes qui vous permettront de vous assurer que tous les logiciels de sécurité présents sur tous les ordinateurs sont à jour et envoient des rapports centralisés dès qu'ils détectent une brèche potentielle.

Vérifiez que votre logiciel de sécurité se met à jour régulièrement et automatiquement : les produits antivirus, anti-spyware et anti-hameçonnage ne sont réellement efficaces que s'ils sont à jour.

Enfin, tenez compte de l'assistance dont vous bénéficiez dans le cadre de la suite logicielle de sécurité que vous avez choisie.

La plupart des petites entreprises ne peuvent pas se permettre de disposer d'une équipe informatique dédiée et, quel que soit le niveau d'expertise de vos collaborateurs, ils n'ont simplement pas le temps d'apprendre à traiter toutes les menaces de sécurité qui peuvent se présenter.

**Pare-feu basé sur l'ordinateur**

De nombreuses personnes pensent que le fait de disposer d'un pare-feu d'entreprise, éventuellement sous forme de périphérique distinct ou intégré à leur routeur Internet, offre une protection adéquate.

Toutefois, les pare-feux de routeur et de dispositifs externes sont généralement moins restrictifs que les pare-feux basés sur des PC, car ils ne comprennent pas toutes les applications qu'un employé individuel doit exécuter et la raison pour laquelle chacune de ces applications peut avoir besoin ou non d'accéder à (ou de télécharger depuis) Internet. C'est la raison pour laquelle les pare-feux de « bordure » sont généralement configurés pour autoriser le passage de la plupart du trafic Web, messagerie, chat, vocal, vidéo ou jeu.

Vous devriez vraiment envisager l'installation d'un pare-feu logiciel sur chaque PC de vos employés, car c'est le seul moyen pour que chaque application utilisée soit examinée, d'abord par l'ordinateur, puis par le pare-feu, pour demander à l'utilisateur si ce logiciel doit ou non être en mesure d'échanger des données avec Internet.

# Processus de sécurité des informations

Cette section passe en revue les mesures concrètes que votre personnel et vous-même devez prendre au quotidien pour vous assurer que les informations de votre entreprise sont protégées

Le fait de disposer de stratégies de sécurité des informations et d'utiliser une bonne technologie de sécurité en ligne contribuera en grande partie à assurer la sécurité des actifs électroniques de votre entreprise. Certaines activités doivent cependant être réalisées manuellement pour vous protéger contre la perte de données.

Les grandes entreprises ont tendance à opter pour les processus de gestion et d'atténuation des risques définis par les normes mondiales de sécurité des informations telles que ISO 27001. Toutefois, en tant que petite entreprise, il est peu probable que vous disposiez du temps et des ressources nécessaires pour appliquer une série de mesures aussi lourdes. Vous devriez donc au minimum essayer de mettre en œuvre les procédures suivantes, même s'il est recommandé de faire l'effort supplémentaire que nécessite l'application de bon nombre des directives ISO 27001 si vous dirigez une entreprise en ligne ou si votre entreprise est régie par un organisme réglementaire.

**Formation à la sécurité**

La plupart des employés n'ont pas besoin d'être des experts de la sécurité, mais il ne faut pas sous-estimer les lacunes de connaissances informatiques de base qui existent chez la plupart des utilisateurs d'informatique lorsqu'ils arrivent dans votre entreprise, même ceux qui viennent d'autres environnements professionnels.

La formation à la sécurité n'a pas à être rigoureuse, mais une session d'une heure consacrée à vos stratégies informatiques et aux bonnes pratiques en matière de sécurité peut contribuer en grande partie à assurer la sécurité de vos données.

Veillez à faire comprendre aux employés qu'ils ne doivent ouvrir que les fichiers provenant d'une source de confiance et qu'il faut absolument identifier et éviter les fichiers exécutables qu'ils pourraient télécharger par inadvertance par e-mail ou par messagerie instantanée.

Si vous ne disposez pas d'un système de gestion centralisé ni d'une équipe informatique pour faire en sorte que tous les PC de vos collaborateurs soient équipés du dernier système d'exploitation, de logiciels et de correctifs à jour, vous devriez former vos employés à vérifier ces éléments par eux-mêmes et à mettre régulièrement à jour leurs logiciels. Si vous ne disposez pas des ressources internes pour dispenser cette formation, n'importe quelle formation peu onéreuse ou financée par le gouvernement pour obtenir le permis de conduire informatique européen ou l'ITQ, couvre ces principes de base.

Si les membres du personnel ont besoin d'un accès « Administrateur » occasionnel sur leur PC pour installer de nouveaux logiciels, assurez-vous qu'ils n'utilisent ces droits administratifs que lorsque c'est approprié, et que leur accès utilisateur est plus restreint dans le cadre de leurs activités quotidiennes.

## Sauvegardes régulières

Songez au préjudice que représenterait pour votre entreprise la perte ou l'indisponibilité de ses informations pendant une période prolongée. Vous risqueriez de voir votre activité bloquée ou de perdre votre réputation auprès de vos clients si vous ne disposez plus des informations qu'ils vous ont confiées.

Les sauvegardes régulières des informations de votre entreprise sont indispensables et, en tant que directeur, vous êtes désormais responsable légalement de tout préjudice survenant dans votre entreprise en raison d'une perte de données.

Dans la mesure du possible, exigez que tous les fichiers, e-mails, code source et autres informations cruciales soient stockés de manière centralisée sur des serveurs que vous contrôlez, afin que vous puissiez vous charger des sauvegardes.

Si vous utilisez un serveur de messagerie ou une base de données, veillez à utiliser un logiciel de sauvegarde conçu pour comprendre ces programmes du serveur au moment de leur sauvegarde afin que, le cas échéant, vous puissiez restaurer des e-mails/enregistrements individuels ou des ensembles de données partiels, au lieu d'avoir à effectuer une sauvegarde instantanée entière.

De même, si votre activité consiste à créer des logiciels, envisagez d'utiliser un logiciel spécialisé de contrôle du code source ou des services en ligne qui comprennent également la structure complexe de ces informations.

Si certains employés doivent travailler à l'extérieur des serveurs de votre entreprise pendant une certaine période et ne peuvent donc pas bénéficier de vos sauvegardes centralisées, assurez-vous qu'ils disposent des moyens, soit sécurisés en ligne, soit par le biais de dispositifs ou de supports de sauvegarde, pour procéder à des sauvegardes régulières de leurs données et de leurs activités.

## Changement des mots de passe

Vous devriez généralement inviter les utilisateurs à changer de mot de passe chaque mois sur tout système utilisé à des fins professionnelles. Si une brèche de sécurité s'est produite à la suite de la découverte d'un mot de passe, mais qu'elle n'a pas été détectée, cela permettra au moins de déterminer une période limitée au terme de laquelle vous pourrez à nouveau être protégé.

Le changement fréquent des mots de passe assure également une protection contre le partage des mots de passe qui, malgré nos stratégies, se produit occasionnellement. Au moins, si un (ex-) employé ou un sous-traitant a connaissance d'un mot de passe qu'il ne devrait pas connaître, cette faille sera à nouveau comblée au bout d'un mois.

Lorsque vous disposez d'un serveur centralisé qui gère certains éléments de sécurité sur chaque ordinateur via une « stratégie de groupe », vous devriez imposer des changements mensuels de mot de passe. Dans tous les cas, vous devriez continuellement rappeler à votre personnel la nécessité de changer de mot de passe chaque mois.

Il est particulièrement important de changer de mot de passe sur tous les systèmes lorsqu'un employé quitte votre entreprise. C'est regrettable à dire, mais les ex-employés peuvent être plus rancuniers qu'il n'y paraît, et rien ne garantit qu'ils ne vont pas entrer au service d'un de vos concurrents.

N'oubliez pas d'autres mots de passe informatiques lorsque vous procédez à ces opérations de changement : les mots de passe utilisés sur les réseaux Wi-Fi (sans fil) sont trop souvent oubliés. Pourtant, il s'agit probablement des mots de passe les plus souvent partagés par des visiteurs de votre entreprise et naturellement, ils peuvent être utilisés à votre insu à quelques mètres seulement des locaux de votre entreprise.

# Stockage des données

Cette section passe en revue les mesures concrètes que votre personnel et vous-même devez prendre au quotidien pour vous assurer que les informations de votre entreprise sont protégées

Le stockage des données est relativement coûteux, de sorte qu'il est préférable de réfléchir soigneusement à votre modèle de sauvegarde et à la durée pendant laquelle il vous faudra conserver chaque sauvegarde. De nombreuses entreprises optent pour le modèle « Grand-père, Père, Fils », dans lequel une sauvegarde différente est effectuée chaque jour, puis une fois par semaine, une sauvegarde étant conservée en tant que sauvegarde hebdomadaire, mais tous les autres supports de sauvegarde étant réutilisés pour l'archivage de la semaine suivante. Puis, chaque mois, l'une des sauvegardes hebdomadaires sort de la rotation indéfiniment pour vous garantir que vous disposerez d'enregistrements instantanés permanents de vos données.

Les sauvegardes régulières devraient être stockées en dehors des locaux de votre entreprise, au cas où ces derniers subiraient un sinistre catastrophique, ou seraient infectés par un logiciel malveillant généralisé ; de plus, les fournisseurs de services Internet sont de plus en plus nombreux à proposer un stockage sécurisé de différents types de sauvegardes « dans le cloud », ce qui vous évite la préoccupation d'éloigner les supports de sauvegarde de votre entreprise pour un stockage sécurisé.

Enfin – la règle d'or absolue – testez le système ! Rien n'est pire que de faire confiance à un système de sauvegarde, pour découvrir plus tard, lorsque vous avez besoin de récupérer des données perdues, que des éléments cruciaux sont manquants. Le tri et la vérification des données de sauvegarde nécessitent du temps et des efforts, mais c'est votre entreprise que vous protégez ainsi.

### Gestion des brèches de sécurité

Malgré vos meilleurs efforts, il peut vous arriver, comme à vos collaborateurs, d'être victime des logiciels malveillants habiles qui continuent à être élaborés par les cybercriminels.

On peut espérer qu'ils soient détectés par l'utilisateur du PC et qu'ils vous soient signalés immédiatement, conformément à votre stratégie. Toutefois, si vous pensez qu'il est possible qu'un logiciel malveillant ait été installé sur le PC d'un utilisateur, la première règle est de déconnecter immédiatement cet ordinateur de tous les réseaux de l'entreprise ainsi que d'Internet.

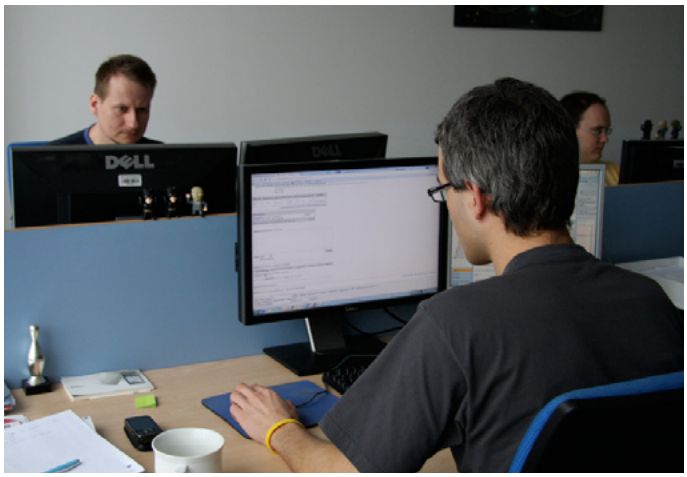
Un « cheval de Troie » ou un logiciel espion implanté dans un PC peut continuer à télécharger des virus depuis Internet ou à échanger des informations aussi longtemps qu'il est connecté à Internet, tandis que de nombreux virus et « vers » continueront à chercher des lieux où se cacher tant qu'ils seront présents sur votre réseau.

Vous devez alors procéder à une évaluation des dégâts. Quels autres équipements, magasins d'informations ou sauvegardes de données de votre entreprise peuvent avoir été compromis ?

Quelles informations importantes de l'entreprise peuvent avoir été perdues ? Quelles informations sensibles de l'entreprise risquent d'avoir été divulguées ? Quelles autres personnes, dans l'entreprise et en dehors, devez-vous informer et par quel moyen ?

Dès que vous aurez pris toutes les mesures pour limiter les dommages et récupérer les informations éventuellement perdues (ou réparer votre réputation), vous devrez récupérer l'ordinateur ou les ordinateurs concerné(s).

En cas de doute au cours du processus de récupération (après tout, nous ne sommes pas tous des experts de l'informatique), demandez l'aide d'un spécialiste, éventuellement par le biais du service de support auquel vous avez fait appel dans le cadre de votre Licence de logiciel de sécurité en ligne, ou auprès d'un centre de réparation informatique local, avant d'affirmer que le problème a été techniquement réparé et d'accepter que l'ordinateur soit reconnecté à tout réseau ou réutilisé dans un cadre professionnel.



# Récapitulatif

Il est incontestablement difficile de lancer une entreprise, puis d'en assurer le fonctionnement fluide et les menaces qui pèsent sur les ordinateurs et les informations électroniques de votre entreprise dans un monde en ligne sont une autre préoccupation pour tout propriétaire de PME.

Toutefois, si vous suivez les étapes simples présentées dans ce document, en adaptant les stratégies, les besoins technologiques et les processus à votre propre entreprise, vous devriez disposer de la sécurité et de la protection nécessaires pour fonctionner avec un minimum d'efforts et de coût.

Fondé en 1991, AVG est un développeur international de pointe dans le domaine des solutions de protection contre les menaces sur Internet destinées aux entreprises et aux particuliers. AVG protège plus de 110 millions d'utilisateurs d'ordinateurs à travers le monde. L'entreprise dispose de bureaux en Europe et en Amérique du Nord et emploie certains des plus grands spécialistes mondiaux de la sécurité Internet, notamment dans le domaine de la recherche, de l'analyse et de la détection des menaces. Les produits primés d'AVG sont distribués dans le monde entier par des revendeurs et disponibles sur Internet. Ils sont en outre proposés par des tiers via des kits de développement de logiciels (SDK, ou Software Development Kits)

AVG SMB group :
bit.ly/AVGSMB

Devenez fan d'AVG:
facebook.com/avgfree

Lisez nos blogs :
blogs.avg.com

Suivez-nous sur :
twitter.com/
officialAVGnews

Devenez un affilié AVG :
avg.com/affiliate

Regardez notre chaîne :
youtube.com/officialAVG


AVG Technologies France
1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com


AVG AU TRAVAIL