experts & décideurs
LES DOSSIERS

TRANSITION DIGITALE
VOTRE ENTREPRISE EST-ELLE PRÊTE ?

CANOPÉE CONSULTING
Expertise comptable & conseil

Membre du groupement France défi
FRANCE DEFI

Au sommaire

France Défi est au cœur de la transition digitale, pour accompagner ses membres experts-comptables et les aider à répondre aux besoins de leurs clients. Une politique qui présente un double objectif : entrer dans le monde d'aujourd'hui et prévenir la cybercriminalité.

TRANSITION DIGITALE : UNE RÉVOLUTION PLEINE DE PROMESSES

Même si toutes les PME n'en ont pas encore pris la pleine mesure, la transition numérique est lancée et rien ne l'arrêtera. Au-delà de l'obligation légale de s'y adapter, la révolution digitale est source d'opportunités.

Encore des efforts… Selon le Digital Economy and Society Index (DESI) publié le 3 mars 2017 par la Commission européenne, la France figure au 16e rang des pays de l'Union en matière de transition numérique. Ce classement pointe notamment, du côté des entreprises hexagonales, un taux d'intégration des technologies numériques inférieur à la moyenne des autres pays de l'Union. « Les grandes entreprises, dont certaines ont été bousculées par l'arrivée de nouveaux acteurs, ont accéléré le mouvement ces dernières années. Dans les PME, les TPE et chez les indépendants, l'évolution est plus lente », analyse Véronique Torner, présidente d'Alter Way, société spécialisée dans les services open source, et membre du Conseil national du numérique (CNNum). Pourtant, comme le relève le classement européen, l'État a donné l'exemple en développant fortement les services dématérialisés. « De nombreuses procédures administratives s'effectuent désormais en ligne, et cette évolution va s'accélérer », assure Philippe Guermeur, directeur associé du cabinet d'expertise comptable 3G Gadras et président de France Défi. Des exemples ? La déclaration sociale nominative (DSN), dont la

SHUTTERSTOCK - SDECORET

Au 16e rang

La France est le mauvais élève de l'UE en termes de transition digitale.

Source : Commission européenne

généralisation interviendra en juillet 2017 (voir « Les trois étapes de la dématérialisation »), et l'obligation pour l'ensemble des fournisseurs de l'État d'établir des factures électroniques à partir de 2020. « De plus en plus de marchés publics ne sont désormais accessibles que par le biais de procédures dématérialisées », complète Véronique Torner. Il en va de même en ce qui concerne les relations avec les banques ou les experts-comptables.

MOINS DE TEMPS PERDU ET UN SUIVI PLUS FIN DE L'ACTIVITÉ

Mise en place d'un système de gestion électronique des documents, définition de procédures de sauvegarde, d'archivage et de sécurisation des données, déploiement de la facturation électronique, sensibilisation des salariés à la cybersécurité… Autant de chantiers à lancer dans le cadre de la transition numérique. Des changements loin d'être anodins, venant bouleverser les habitudes. D'où certaines hésitations. « Il est parfois nécessaire de se former, mais les outils destinés aux entreprises sont de plus en plus intuitifs, de plus en plus simples à utiliser », modère Philippe Guermeur. À la clé, il y a de nombreux effets bénéfiques, comme les gains de temps liés à l'automatisation de certaines tâches répétitives sans aucune plus-value. « Et, dans une PME, où le temps est compté, c'est précieux. C'est autant de plages libérées pour s'occuper de ses clients, aller visiter un chantier, prospecter ou échanger avec ses collègues. Bref, pour se concentrer sur son cœur de métier », constate Philippe Guermeur. Autre impact positif, le suivi plus étroit de l'activité. « Certaines solutions permettent de disposer de tableaux de bord quotidiens sur lesquels apparaissent en temps réel le volume de l'activité ou le montant des encaissements, ce qui simplifie le pilotage », note encore Philippe Guermeur.

> *« Il est parfois nécessaire de se former, mais les outils destinés aux entreprises sont de plus en plus intuitifs, de plus en plus simples à utiliser »*
>
> ***Philippe Guermeur, directeur associé du cabinet d'expertise comptable 3G Gadras et président de France Défi***

LE POTENTIEL DE LA CROISSANCE CONNECTÉE

Automatiser les actes de gestion quotidienne, c'est bien. Offrir des opportunités de développement, c'est encore mieux. « Le numérique représente un gisement important de croissance, encore faut-il l'exploiter », remarque Véronique Torner. Site vitrine ou de e-commerce, présence sur une plateforme, valorisation de son activité sur les réseaux sociaux… Autant de leviers qu'il est possible d'activer. « Industriels, artisans, commerçants, prestataires de services, indépendants… Chacun à son niveau peut trouver un intérêt commercial à se rendre plus visible », assure Véronique Torner. Une démarche d'autant moins risquée que les investissements requis restent mesurés. Et les résultats sont parfois surprenants. « L'un de mes clients, présent sur un marché de niche et employant quatre salariés, a vu son chiffre d'affaires multiplié par deux en cinq ans en se lançant dans le e-commerce », raconte Philippe Guermeur. Une ouverture sur le monde qui, grâce à un référencement efficace, a permis à cette petite société d'engranger des commandes des quatre coins de la planète. Une réussite loin d'être unique. ■

Jean-Marc Engelhard

TROIS ÉTAPES DE LA DÉMATÉRIALISATION ADMINISTRATIVE DES ENTREPRISES

LA DSN

Destinée à simplifier les démarches administratives des entreprises, la déclaration sociale nominative (DSN) a concerné les grandes entreprises dès 2015. Elle sera généralisée en juillet 2017, date à laquelle les TPE et les PME auront également l'obligation de transmettre leurs données sociales mensuelles sous cette forme dématérialisée.

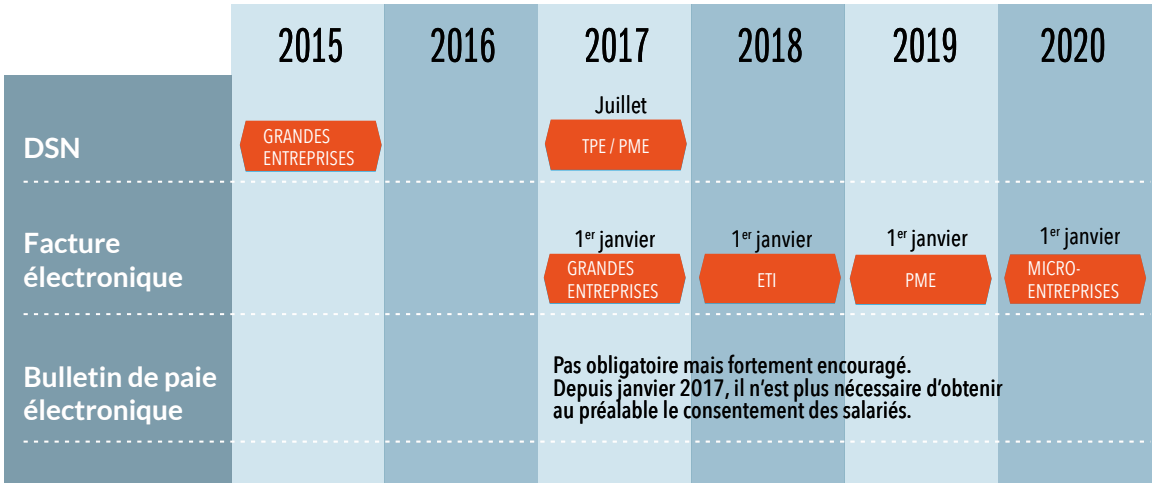
LA FACTURE ÉLECTRONIQUE

De manière progressive, la facturation électronique s'impose pour les marchés conclus avec l'État, les collectivités territoriales et les établissements publics. Obligatoire pour les grandes entreprises depuis le 1er janvier 2017, elle va s'étendre aux ETI (1er janvier 2018), aux PME (1er janvier 2019) puis aux micro-entreprises (1er janvier 2020). Parallèlement, suivant le même calendrier, les entreprises auront l'obligation d'accepter les factures électroniques de leurs fournisseurs.

LE BULLETIN DE PAIE ÉLECTRONIQUE

Si la transmission des feuilles de paie par voie électronique n'est pas obligatoire, elle est fortement encouragée : depuis janvier 2017, il n'est plus nécessaire d'obtenir au préalable le consentement des salariés.

Jean-Marc Engelhard



LA DIGITALISATION, OUI LA CYBERCRIMINALITÉ, NON

France Défi a lancé un Observatoire de la cyberprévention. Son but : analyser les causes et les sources des attaques

Renault, Fedex, Telefonica… Le virus WannaCry a inscrit à son tableau de chasse au moins 200 000 victimes dans 150 pays. Une attaque informatique d'ampleur mondiale qui a rappelé aux entreprises que la cybercriminalité est désormais une menace majeure. Fuite de données, vol de fichiers clients, blocage d'activité, les pirates peuvent user de différentes méthodes. Les grands groupes ne sont pas les seuls dans la ligne de mire. Moins bien protégées, moins conscientes des risques, les PME constituent des cibles de choix. Pour mieux identifier les dangers et conseiller leurs clients, le groupement d'experts-comptables France Défi a lancé un Observatoire de la cyberprévention. Son but : analyser les causes et les sources des attaques pour déterminer les préjudices causés et les réponses à apporter. Sa première enquête menée sur l'ensemble des 129 cabinets France Défi, qui totalisent plus de 100 000 entreprises clientes, révèle que, sur les six derniers mois, plus de 40 % d'entre elles ont subi au moins une cyberattaque. Une action qui se traduit par un préjudice d'exploitation dans 59 % des cas. Mais 39 % des entreprises sont également touchées au portefeuille. Un diagnostic qui permet à l'Observatoire d'édicter de grands principes à respecter. En premier lieu, établir obligatoirement un plan de sauvegarde : pour 68 % des sociétés, les menaces ont été déjouées notamment grâce à la restauration de ces sauvegardes révèle l'enquête. D'autres précautions sont nécessaires comme l'adoption de mots de passe robustes, d'un antivirus, d'un firewall à jour et d'un antispam. Pour une sécurité renforcée, d'autres actions peuvent être mises en place : élaborer un plan de reprise et de continuité d'activité, souscrire un contrat d'assurance cyber, créer un test d'intrusion et surtout sensibiliser les collaborateurs. Une mesure indispensable car, selon l'Observatoire, dans plus de 65 % des cas, la source de l'attaque est due à la négligence d'un collaborateur.

SHUTTERSTOCK - FARKNOT ARCHITECT

+de 40%

des entreprises suivies par l'Observatoire ont subi une attaque dans les six derniers mois.

Source : Observatoire de la Cyberprévention France Défi

1 COLLECTER
HÉBERGER
ARCHIVER
SÉCURISER
PRÉVENIR ET ASSURER

GED : QUATRE ÉTAPES POUR DÉMATÉRIALISER VOS DOCUMENTS

Tri dans les archives, choix d'un outil de gestion des documents adapté, installation du matériel nécessaire aux salariés… Ce sont quelques-unes des étapes pour passer au tout-numérique.

Transformer ses documents papier en fichiers numériques ? La dématérialisation est une option dans l'air du temps. Elle va progressivement s'imposer, en raison de ses nombreux avantages. « Elle a simplifié la tâche des commissaires aux comptes. Fini les longues séances à la photocopieuse et les encombrants classeurs, désormais tout est scanné », raconte ainsi Christian Rotureau, expert-comptable et commissaire aux comptes au sein du cabinet AEC, à Sarlat, membre du groupement France Défi. « En quelques secondes, il est possible d'avoir sous les yeux tout l'historique de ses relations avec un client », renchérit Pascal Guicherd, responsable de MG Systèmes d'information, une filiale du cabinet d'expertise comptable rhônalpin MG, membre de France Défi, spécialisée dans l'installation et la maintenance de postes de travail et de logiciels. « Sans compter la réduction de certains coûts, comme ceux liés à la consommation de papier, à l'envoi des factures ou à l'espace nécessaire au stockage des documents », ajoute Christian Rotureau.

SÉLECTIONNER LES DOCUMENTS AVANT DE LES DÉMATÉRIALISER

Chez AEC, la dématérialisation s'est inscrite dans le cadre de la certification environnementale ISO 14001. « Nous l'avons mise en place par paliers, service par service », explique Christian Rotureau.

SHUTTERSTOCK - ILIKESTUDIO

57 %

des entreprises en France ont recours à l'échange de données informatisées (EDI).

Source : Eurostat, enquête communautaire sur les TIC 2015.

« Avant de se lancer, une sélection doit être effectuée dans les archives. Certains documents doivent être sauvegardés, parce qu'il ont un intérêt professionnel réel ou qu'il existe une obligation légale de conservation », relève de son côté Pascal Guicherd. Attention à ne pas créer un « cimetière de données », dont la plus grande partie aura été scannée pour rien, puisqu'elle ne sera jamais réutilisée.
La perspective de la dématérialisation est donc en pratique une occasion de revoir ses méthodes de classement. Avant même d'opter pour une solution ou une autre, une phase préalable s'avère indispensable : la définition de l'arborescence. « Que doit-on classer et où ? Cette phase de réflexion est essentielle pour qu'elle corresponde bien aux attentes des collaborateurs », souligne Pascal Guicherd. La gestion électronique de documents (GED) est un élément fédérateur dans l'entreprise, elle doit obtenir l'assentiment de tous les utilisateurs. Il peut donc s'avérer utile d'associer les salariés des différents services à la conception de cette méthode de classement.

> *« Fini les longues séances à la photocopieuse et les encombrants classeurs, désormais tout est scanné »*
>
> ***Christian Rotureau, expert-comptable et commissaire aux comptes au sein du cabinet AEC, membre du groupement France Défi***

CHOISIR UN LOGICIEL DE GED ADAPTÉ

Sur le marché, il existe une multitude de logiciels de gestion électroniques des documents (GED), indispensable pour la dématérialisation et l'archivage. Il n'est pas toujours opportun d'opter pour l'outil le plus sophistiqué, l'important étant que l'indexation et la recherche soient les plus intuitives et les plus rapides possible (pour en savoir plus, lire « GED : trois critères pour choisir sa solution »).

S'ÉQUIPER DU BON MATÉRIEL

Pour que les salariés adoptent la gestion électronique des documents, encore faut-il qu'ils soient équipés du matériel adéquat. « C'est un critère de réussite du passage à la dématérialisation », assure Pascal Guicherd. À mettre sur sa liste : des écrans d'ordinateur de grande taille (voire deux par poste de travail pour certaines activités), des scanners de production individuels sans oublier un logiciel de lecture des PDF permettant d'intervenir directement sur les documents.

OUVRIR SON OUTIL DE GED À SES CLIENTS

La plupart des logiciels de GED permettent de donner des droits d'accès à ses clients. « Ainsi, ces derniers peuvent consulter les documents les concernant 24 heures sur 24. Cette fonctionnalité favorise aussi les relations collaboratives. Par exemple, dans la construction, le fait que les différents corps de métier puissent accéder aux documents d'un chantier, les actualiser et en déposer de nouveaux, est facteur de fluidité », explique Pascal Guicherd. Évidemment, le passage à la dématérialisation implique, si ce n'est déjà fait, la mise en place d'une solide stratégie de sauvegarde des données. Indispensable pour qui veut s'éviter des sueurs froides. ■

Jean-Marc Engelhard

GED : TROIS CRITÈRES CLÉS POUR CHOISIR SA SOLUTION

Lors du choix d'un logiciel de gestion électronique des documents (GED), le prix est loin de constituer l'élément sur lequel se focaliser. Voici trois autres critères de choix pour éviter les mauvaises surprises.

« Zéro papier ! » Pour parvenir à cet objectif, la gestion électronique des documents (GED) est une alliée indispensable. En la matière, il existe une multitude d'offres, à tous les prix. « Il n'existe pas de logiciel idéal et pas de leader. Certains sont plus adaptés aux petites entreprises, d'autres s'adressent à certains secteurs d'activité. Bref, le choix est lié aux besoins de chaque entreprise », prévient Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre du groupement France Défi.

GED : PRIVILÉGIER DES OUTILS SIMPLES

Il existe une multitude de solutions de gestion électronique des documents, plus ou moins sophistiquées. « Mais ce qui conviendra à une grande entreprise ne sera pas adapté à une TPE », souligne Pascal Guicherd. « Mieux vaut opter pour une solution simple, intuitive, ne nécessitant pas des journées de formation avant la première utilisation. Une trop grande technicité risque de décourager les collaborateurs », insiste Pascal Guicherd. Seuls points non négociables : la possibilité d'ajouter des fonctionnalités si nécessaire et l'importance du volume de stockage, puisqu'au fil du temps la masse de docu-

SHUTTERSTOCK - EVERYTHING POSSIBLE

7%

des intentions d'achats progiciels 2017sont dédiés aux GED et à la dématérialisation.

Source : Celge.fr

ments ne va cesser d'augmenter. La facilité à intégrer tous types de documents, quels que soient leur format informatique et leur provenance, est également à ne pas négliger.

OPTER POUR UNE SOLUTION INDÉPENDANTE

« En revanche, il faut choisir un produit indépendant de tout matériel ou de tout logiciel », souligne Pascal Guicherd. La plupart des éditeurs de logiciels « métiers », par exemple dans le domaine de la gestion ou de la comptabilité, proposent leurs propres outils de GED. La proposition est séduisante, mais qu'en sera-t-il lorsque vous souhaiterez changer de fournisseur et récupérer les données stockées depuis plusieurs années ? Ce n'est pas forcément vers ces solutions qu'il faut se diriger. « Le risque, avec ces solutions "chaînées", est d'en devenir captif. Que se passe-t-il si l'entreprise souhaite se passer du logiciel auquel est lié l'outil de GED ? », s'interroge Pascal Guicherd.

SE PENCHER SUR LES CONDITIONS DE RÉVERSIBILITÉ

Avant de faire son choix, les clauses de réversibilité doivent être examinées de près. En clair, il s'agit de vérifier les possibilités et les modalités de récupération des données, notamment en cas de changement de prestataire, car elles peuvent parfois être très restrictives ou complexes à mettre en œuvre. « Sous quel format sont-elles rendues ? Le contrat prévoit-il des conditions limitatives ? Quelles sont les conditions financières ? », liste Pascal Guicherd. À défaut d'indépendance du prestataire, il est recommandé de prévoir une clause de réversibilité très précise, détaillant les modalités de récupération des documents. Un moyen de se prémunir contre les mauvaises surprises : certains prestataires autorisent par exemple la récupération des données, mais fichier par fichier… De quoi décourager les meilleures volontés. ■

Jean-Marc Engelhard

> « Il n'existe pas de logiciel idéal et pas de leader. Certains sont plus adaptés aux petites entreprises, d'autres s'adressent à certains secteurs d'activité. Bref, le choix est lié aux besoins de chaque entreprise »
>
> ***Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre du groupement France Défi***

LA FACTURE ÉLECTRONIQUE BIENTÔT POUR TOUS

Si de nombreuses entreprises procèdent encore à la saisie manuelle de leurs factures et à leur envoi par courrier postal, cette manière de faire est vouée à disparaître.

« Le législateur est en train d'imposer progressivement la dématérialisation des factures à toutes les entreprises », explique Pierre Billet, associé chez Axens, membre de France Défi.

LA FACTURE ÉLECTRONIQUE OBLIGATOIRE D'ICI À 2020

La loi pour la croissance, l'activité et l'égalité des chances économiques du 6 août 2015 oblige ainsi les entreprises à accepter la facture électronique selon un calendrier progressif. Les grandes entreprises doivent se plier à cette nouvelle obligation depuis le 1er janvier 2017, les ETI le feront pour le 1er janvier 2018 et les PME au 1er janvier 2019, tandis que les entreprises de moins de 10 salariés auront jusqu'au 1er janvier 2020 pour s'y conformer.
« Cela va les contraindre progressivement à utiliser des logiciels capables d'établir des factures sous un format dématérialisé (PDF…) et très vraisemblablement, à court terme, sous un format standardisé d'échange de données, le format EDI, pour Échange de données informatisé », décrypte l'expert-comptable. Il s'agit d'une forme d'échange de documents sécurisé et traçable, déjà utilisée par les banques mais aussi les experts-comptables pour la transmission des liasses fiscales à l'administration.

SHUTTERSTOCK - ANDREY_POPOV

30%

du temps des services comptables était consacré à la saisie manuelle des factures fournisseurs en 2010.

Source : étude IDC citée par le ministère de l'Economie

UN MEILLEUR CONTRÔLE DES FACTURES

Pour l'État, l'intérêt est notamment de pouvoir mieux contrôler l'exhaustivité des factures. « Alors qu'avec du papier, il peut être difficile de prouver qu'il manque une facture, l'administration fiscale pourra, grâce à la simple extraction des journaux des échanges EDI, où tout sera daté, numéroté et enregistré, vérifier qu'il n'y a pas eu de suppression ou de modification des factures », explique l'expert-comptable.

Plus largement, cette dématérialisation sera sans doute synonyme d'une vraie révolution pour les entreprises. « Pour elles, la vraie question à se poser est de voir comment transformer cette contrainte en une opportunité de gagner du temps dans la saisie des achats et des ventes. À terme, on peut imaginer la mise en place de plateformes sur lesquelles seront saisies les données et les factures générées et envoyées aux différents clients référencés puis réceptionnées, pointées et intégrées à la comptabilité de manière automatique », anticipe Pierre Billet.

> *« Il s'agit de voir comment transformer cette contrainte en une opportunité de gagner du temps dans la saisie des achats et des ventes »*
>
> ***Pierre Billet, associé chez Axens, membre du groupement France Défi***

LA FIN DE CERTAINES LATITUDES

Si le passage à un tel système peut effectivement permettre de réduire le temps alloué à des tâches à faible valeur ajoutée comme la saisie manuelle des factures fournisseurs, qui, selon des études citées par le gouvernement, monopolise 30 % du temps des services comptables, il représente aussi la fin d'une certaine souplesse de gestion pour les entreprises. Il ne sera ainsi plus possible de jouer sur les dates de traitement des factures, par exemple pour gérer sa trésorerie. Du côté des services comptables ou des cabinets d'expertise comptable, ce sont les missions de saisie et sans doute certaines déclarations liées, qui sont vouées à disparaître.

BIEN SE PRÉPARER AU PASSAGE À LA FACTURE ÉLECTRONIQUE

Pour l'heure, les entreprises doivent surtout s'assurer de pouvoir se conformer à leurs nouvelles obligations en s'équipant d'un système EDI. « C'est une simple mise en écriture informatique compressée des données. Tous les éditeurs de logiciels de facturation ou de gestion commerciale vont probablement le proposer très rapidement. Pour les entreprises qui en disposent déjà, il faudra être vigilant sur leur mise à jour et pour celles qui établissent leurs factures sur papier ou sur tableur il faudra s'en doter », précise Pierre Billet. Une première étape avant de réfléchir plus globalement aux évolutions nécessaires en termes d'organisation et de gestion. ■

Marion Perrier

PASSER AU BULLETIN DE PAIE DÉMATÉRIALISÉ

Afin d'encourager les entreprises à recourir à la feuille de paie électronique, de nouvelles règles s'appliquent depuis janvier 2017. Une étape supplémentaire vers le « zéro papier », synonyme d'économies.

La remise du bulletin de paie dans une enveloppe de la main à la main ou envoyé par courrier appartiendra-t-elle bientôt au passé ? Pas sûr car, aujourd'hui, contrairement à leurs homologues allemandes ou britanniques, peu d'entreprises françaises ont opté pour la dématérialisation de ce document remis tous les mois à leur personnel. « Pourtant, la dématérialisation se traduit par des économies liées au coût de l'impression et du timbre pour l'envoi et par un gain de temps lié à la mise sous pli », remarque Alexandra Despres, responsable du service social au sein du cabinet d'expertise comptable Michel Creuzot (Orléans), membre de France Défi, qui vient d'opter pour cette formule. Selon le rapport « Pour une clarification du bulletin de paie » publié par le ministère du Travail en juillet 2015, ce gain atteindrait entre 10 et 32 centimes par feuille de paie. À multiplier par 12 et par le nombre de salariés…

DES RÈGLES DE CONSERVATION DU BULLETIN DE PAIE ENCADRÉES

Afin d'accélérer le mouvement, de nouvelles règles, fixées par un décret du 16 décembre 2016, sont entrées en vigueur le 1er janvier. La première ? « Il n'est plus nécessaire d'obtenir au préalable

SHUTTERSTOCK - ANTONIO GUILLEM

10 à 32 cts

économisés par feuille de paie émise.

Source : ministère du Travail

le consentement des salariés. Il faut en revanche, un mois avant la mise en place de cette nouvelle procédure, les en informer par courrier recommandé avec accusé de réception, en leur rappelant leur droit d'opposition. Et également avertir les nouveaux embauchés », précise Alexandra Despres. Des règles encadrent strictement l'accès à ces documents (lire ci-dessous). Et si l'entreprise cesse son activité, elle doit informer les salariés au moins trois mois avant la fermeture du service où les bulletins sont centralisés. De plus, pas question de proposer une solution d'accès complexe : les collaborateurs doivent pouvoir récupérer, à tout moment, l'intégralité de leurs bulletins de paie, sans manipulation complexe ou répétitive, et dans un format électronique structuré et couramment utilisé. Les mêmes règles s'appliquent en cas de stockage chez un prestataire. « Nous avons décidé de mettre à disposition des collaborateurs du cabinet un coffre-fort électronique dans lequel leur sera envoyé leur bulletin de paie et où ils pourront rassembler tous leurs documents administratifs », explique Alexandra Despres. Dernière exigence, les feuilles de paie devront aussi être consultables via le compte personnel d'activité (CPA) récemment mis en place. ■

Jean-Marc Engelhard

> *« Il n'est plus nécessaire d'obtenir au préalable le consentement des salariés. Il faut en revanche, un mois avant la mise en place de cette nouvelle procédure, les en informer »*
>
> ***Alexandra Despres, responsable du service social au sein du cabinet d'expertise comptable Michel Creuzot, membre de France Défi***

7 REPÈRES POUR METTRE EN PLACE LE BULLETIN DE PAIE ÉLECTRONIQUE

1. LES OBLIGATIONS DE L'EMPLOYEUR PRÉALABLES À LA DÉMATÉRIALISATION DES BULLETINS DE PAIE

L'employeur qui souhaite dématérialiser les bulletins de paie du personnel doit au préalable :

- s'assurer du respect des garanties exigées (intégrité et confidentialité des données, durée minimale de mise à disposition des bulletins, possibilité pour le salarié de récupérer l'intégralité de ses bulletins de paie à tout moment) ;
- informer, au moins un mois avant, chaque salarié de la décision de dématérialiser les bulletins de paie et de leur droit d'opposition ;
- après la réalisation de chaque paie, s'assurer de la mise à disposition des bulletins de paie sur le compte personnel d'activité, selon des modalités pratiques qui restent à déterminer.

2. LE DROIT D'OPPOSITION DU SALARIÉ

L'employeur peut dématérialiser le bulletin de paie, sauf si le salarié s'y oppose. Le salarié peut faire part de son opposition à tout moment. Dans ce cas, l'employeur doit, pour le salarié demandeur, revenir au bulletin de paie « papier » dans les meilleurs délais, et au plus tard trois mois après la demande du salarié.

3. LA DURÉE DE DISPONIBILITÉ

Sous la forme électronique, le bulletin de paie doit être disponible :

- soit pendant 50 ans ;
- soit jusqu'à ce que le salarié ait atteint 75 ans.

4. L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DES DONNÉES

Comme auparavant, l'employeur doit garantir l'intégrité des données figurant sur le bulletin de paie. En outre, à compter du 1er janvier 2017, il doit également garantir leur confidentialité.

5. L'ACCESSIBILITÉ DES BULLETINS DÉMATÉRIALISÉS

L'employeur doit assurer l'accessibilité des bulletins dématérialisés dans le cadre du compte personnel d'activité (CPA).
Le CPA permettra de consulter les bulletins de paie ; toutefois, c'est l'employeur ou un prestataire choisi par l'employeur qui en assure la conservation, et non le CPA.

6. LES RISQUES ENCOURUS PAR L'EMPLOYEUR

Le non-respect des dispositions relatives au bulletin de paie dématérialisé est puni d'une contravention de 3e classe, c'est-à-dire d'une amende pouvant aller jusqu'à 450 € pour les personnes physiques et 2 250 € pour les personnes morales.

7. LA DATE D'ENTRÉE EN VIGUEUR

1er janvier 2017

ECS

EN SAVOIR PLUS

Article 54 de la loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels
Décret n° 2016-1762 du 16 décembre 2016 relatif à la dématérialisation des bulletins de paie et à leur accessibilité dans le cadre du compte personnel d'activité.

2

COLLECTER
HÉBERGER
ARCHIVER
SÉCURISER
PRÉVENIR ET ASSURER

SERVEUR INTERNE : DES ATOUTS, PEU DE CONTRAINTES

Alors que certaines entreprises font appel à un hébergeur, d'autres préfèrent recourir à un serveur interne. Un choix garantissant leur indépendance et impliquant peu de contraintes.

Préserver son indépendance et ne pas dépendre d'un prestataire, telles sont les raisons principales pour lesquelles l'expert-comptable Hervé Mabileau a choisi d'équiper son cabinet, Abaq Conseil et Expertise comptable, membre du groupement France Défi, d'un serveur informatique en interne. Mais cette solution en local présente bien d'autres avantages. « Il y a un aspect financier non négligeable. Disposer de son propre serveur revient jusqu'à trois fois moins cher que les services d'un hébergeur, assure Hervé Mabileau. Par ailleurs, il est plus simple de négocier le prix des logiciels lorsque l'on n'est pas déjà engagé avec le fournisseur qui les commercialise. » Reste que cette option n'est pas adaptée à tout type de structure. Par exemple, dans le cas d'une activité commerciale dispersée dans différents points de vente, l'hébergement des données sur un serveur externe s'impose. En revanche, la solution locale convient tout à fait à des entreprises monosites. « C'est le cas de petites sociétés industrielles ayant recours à des logiciels très pointus, ne pouvant fonctionner en mode hébergé », précise Hervé Mabileau.

UNE SOLUTION FAVORISANT L'AGILITÉ

Recourir à un serveur local permet aussi de s'affranchir des contraintes liées à Internet, en cas de dysfonctionnement ou de

SHUTTERSTOCK - DMITRY KALINOVSKY

12,7 MDS $

le marché mondial des serveurs est néanmoins en baisse (-5,8%) face au Cloud public.

Source : Gartner, juin 2017

panne momentanée du réseau notamment. «Même sans Internet, il est possible d'accéder à ses logiciels et à ses données, et donc de continuer à travailler», constate Hervé Mabileau. En prime, l'agilité est de mise : lorsque le système d'information dépend d'un réseau interne, il est facile de déployer rapidement deux ou trois postes de travail supplémentaires pour accueillir de nouveaux collaborateurs.

S'ENTOURER DES BONNES COMPÉTENCES

Bref, la solution interne présente de nombreux avantages, mais elle entraîne aussi quelques contraintes, en particulier la nécessité de mettre en place, avec l'aide d'une société spécialisée, une procédure efficace de sauvegarde et de restauration des données. «Il existe des solutions de sauvegardes quotidiennes entièrement automatisées», rassure Hervé Mabileau. Par ailleurs, impossible de se passer d'un prestataire susceptible d'intervenir en cas de dysfonctionnement ou d'intégration de nouvelles fonctionnalités. Et celui-ci doit être choisi avec soin. Par exemple, pour une PME, mieux vaut se diriger vers des sociétés à taille humaine. Chez un géant de la maintenance, ses demandes risquent de ne pas être jugées prioritaires. Il est tout aussi nécessaire de désigner, en interne, un référent à qui il revient de gérer le serveur au quotidien, voire d'installer de nouveaux logiciels. Du reste, rien n'empêche de faire cohabiter un serveur interne avec des services en ligne, notamment pour les entreprises qui doivent donner la possibilité à leurs clients d'accéder à certaines informations contenues sur le serveur. Une tendance qui ne cesse de se développer. ■

Jean-Marc Engelhard

> « Même sans Internet, il est possible d'accéder à ses logiciels et à ses données, et donc de continuer à travailler »
>
> ***Hervé Mabileau, gérant du cabinet Abaq Conseil et Expertise comptable, membre du groupement France Défi***

CLOUDS GRAND PUBLIC : FIABLES POUR LES ENTREPRISES AUSSI ?

Dropbox, OneDrive, GoogleDrive, iCloud… ces solutions de stockage familières des particuliers peuvent également être utilisées par les entreprises. Mais utiliser un cloud demande certaines précautions.

Photos de vacances, vidéos de famille, morceaux de musique, documents administratifs… De nombreux particuliers utilisent des solutions en cloud pour stocker leurs documents. Le plus souvent gratuites, accessibles de partout et de n'importe quel appareil connecté, tout en évitant de saturer la mémoire de son smartphone ou de son ordinateur personnel, les solutions de stockage en ligne s'avèrent particulièrement séduisantes. Mais sont-elles vraiment appropriées à l'archivage des documents d'entreprise ? « Elles sont adaptées au fonctionnement de beaucoup d'entreprises, pour partager des documents entre collègues et avoir un accès à ses données où que l'on se trouve, mais à condition de respecter certaines règles », explique Fabien Corneillie, associé, en charge du pilotage du système d'information au cabinet d'expertise comptable CTN France, membre du groupement France Défi.

SHUTTERSTOCK - RAWPIXEL.COM

17 %

des entreprises utilisent le cloud en France pour leur stockage mais aussi leurs logiciels.

Source : Eurostat, enquête communautaire sur l'usage des TIC et le commerce électronique.

CLOUD : OPTER POUR UN FOURNISSEUR RECONNU

Avant d'adopter une solution, se pencher sur les conditions d'utilisation est impératif. Rébarbatif certes, mais c'est le meilleur moyen d'éviter les mauvaises surprises. Ainsi, vérifier les lieux où les données sont stockées ou celui où le fournisseur est établi n'est pas inutile : ils détermineront le droit applicable et les tribunaux compétents en cas de litige. Par exemple, si les serveurs de votre prestataire sont aux États-Unis, il faut savoir que les autorités américaines ont la possibilité, conformément au Patriot Act, de consulter et de copier vos données. Cela reste une éventualité infime mais réelle. « Par ailleurs, il est préférable de choisir un outil à la réputation bien établie, pour être assuré de la pérennité de ses données et ne pas se retrouver avec un fournisseur disparaissant sans préavis », assure Fabien Corneillie.

ÉVITER LES SOLUTIONS GRATUITES

De nombreuses offres cloud sont gratuites. Outre le fait que leur capacité de stockage est réduite, et donc rarement suffisante pour une entreprise, ce n'est pas la seule raison de préférer une solution payante. « Rien n'étant jamais gratuit, ces offres autorisent, en contrepartie, la possibilité pour le fournisseur d'accéder aux données pour les analyser », pointe Fabien Corneillie. Mieux vaut donc se tourner vers des solutions professionnelles comme Dropbox Business ou OneDrive Entreprise. En plus de systèmes de sécurité avancés, ces dernières offrent de nombreuses fonctionnalités supplémentaires. Par exemple, la possibilité de définir des droits d'accès ou d'effacer à distance des fichiers contenus dans un appareil perdu ou volé.

QUID DES DONNÉES SENSIBLES ?

Placer dans le cloud des informations liées à un projet dans le domaine de la défense ou soumis à un accord de confidentialité ? Pas vraiment recommandé, sauf à crypter l'ensemble des données concernées à un niveau très élevé. « Pour les documents les plus sensibles, un coffre-fort numérique constitue la solution en ligne la mieux sécurisée », remarque Fabien Corneillie. Un haut niveau de protection lié au fait que les données qu'il contient sont cryptées dès leur envoi et le restent même lorsqu'elles sont consultées. Comme pour les fournisseurs du cloud, mieux vaut opter pour un fournisseur reconnu. ■

Jean-Marc Engelhard

> « Il est préférable de choisir un outil à la réputation bien établie, pour être assuré de la pérennité de ses données et ne pas se retrouver avec un fournisseur disparaissant sans préavis »
>
> ***Fabien Corneillie, associé, en charge du pilotage du système d'information au cabinet d'expertise comptable CTN France, membre du groupement France Défi***

QUATRE CRITÈRES POUR CHOISIR SON HÉBERGEUR DE DONNÉES

Confier à un prestataire le soin de conserver l'ensemble de ses données, voire de gérer à distance l'ensemble de son système d'information, c'est une décision stratégique. Voilà quatre points à vérifier avant de signer un contrat.

• LE LIEU DE STOCKAGE DES DONNÉES

Des hébergeurs excellents, il y en a partout dans le monde. Pourtant, mieux vaut privilégier un prestataire européen. La raison ? « Lorsque les données sont hébergées hors de l'Union européenne, les entreprises ont obligation d'en informer leurs clients », explique Michel Guillout, responsable informatique et qualité du cabinet d'expertise comptable Cigeco, membre du groupement France Défi. Une préférence dictée également par le fait que la réglementation appliquée aux données est celle du pays où elles sont stockées. Aux États-Unis, par exemple, le Patriot Act autorise l'administration américaine à accéder, sous conditions, aux données informatiques des entreprises et des particuliers. Cela dit, les grands acteurs américains de l'hébergement ne conservent pas forcément les données outre-Atlantique car ils disposent de data centers en Europe. À vérifier avant de signer un contrat, en n'oubliant pas les lieux de conservation lorsque, par sécurité, le stockage est répliqué sur plusieurs serveurs… Michel

SHUTTERSTOCK - WATCHARAKUN

156

datacenters recensés en France.

Source : étude Xerfi 2017

Guillout suggère de privilégier des sites français. « En raison d'une législation particulièrement stricte en matière de protection des données et d'un contrôle rigoureux des prestataires », précise-t-il.

LE SYSTÈME DE SAUVEGARDE ET LES MODALITÉS DE RÉVERSIBILITÉ

D'autres sujets doivent être pris en compte dans les offres des hébergeurs. Les sauvegardes régulières vont de soi, mais pas forcément la conservation des états successifs d'un même fichier. « Or il peut être utile de disposer de plusieurs versions, enregistrées à des dates différentes », pointe Michel Guillout. Essentiel également, les conditions de la réversibilité des données, autrement dit la capacité à les récupérer. « Les modalités doivent pouvoir être mises en œuvre simplement et rapidement », insiste Michel Guillout. Mieux vaut donc qu'elles soient précisément décrites dans le contrat.

LA GARANTIE DE LA DISPONIBILITÉ DES DONNÉES

Être certain de pouvoir disposer en permanence d'un accès à ses données est un impératif. Une garantie que donnent la plupart des leaders de l'hébergement, comme Orange, Google, 1and1, OVH ou Ipgarde. « Cette garantie de disponibilité peut être complétée par un engagement de délai de rétablissement de l'accès en cas d'incident », précise Michel Guillout. Dans le même temps, il faut aussi s'assurer que l'hébergeur bénéficie d'accords avec les principaux opérateurs Internet.

LA SÉCURISATION DES CONNEXIONS

Si les data centers sont généralement très sécurisés, la qualité de la protection des données « en transit » peut varier. « Cependant, généralement, les hébergeurs reconnus proposent des connexions sécurisées et un cryptage lors des transferts de fichiers », relève Michel Guillout. Reste enfin à vérifier que le prestataire dispose de certifications et d'attestations faisant autorité dans le domaine de la sécurité numérique et qu'il bénéficie de la norme ISO 27001. C'est la garantie d'un système efficace de protection des informations. ■

Jean-Marc Engelhard

> « Privilégier les sites français en raison d'une législation particulièrement stricte en matière de protection des données et d'un contrôle rigoureux des prestataires »
>
> ***Michel Guillout, responsable informatique et qualité du cabinet d'expertise comptable Cigeco, membre du groupement France Défi***

COLLECTER
HÉBERGER
3 ARCHIVER
SÉCURISER
PRÉVENIR ET ASSURER

DONNÉES DE L'ENTREPRISE : QUELLE DURÉE DE CONSERVATION ?

Pour chaque type de documents, la législation prévoit une durée de conservation minimale. Que ces données soient archivées en version papier ou numérisées, le délai est identique la plupart du temps.

Conserver ses données en version numérique ? Retenir cette option n'a en fait presque aucune incidence sur leur durée de conservation. « Elle est identique, à une exception près, explique Romain Caffier, expert-comptable au sein du cabinet 3G Gadras, membre du groupement France Défi. Si les contrats conclus dans le cadre d'une relation commerciale doivent être conservés durant cinq ans, les contrats conclus par voie électronique avec des particuliers doivent, eux, l'être pendant dix ans. » Rien n'interdit cependant de les archiver plus longtemps. « Qu'il s'agisse de l'achat d'un fonds de commerce ou de parts sociales, les titres de propriété et les actes de vente doivent être conservés à vie », recommande d'ailleurs Romain Caffier. À ne pas négliger non plus, la date à partir de laquelle le délai commence à courir. « Pour les contrats commerciaux, il débute lorsqu'ils sont rompus. Pour les bulletins de paie, c'est à partir du moment où le salarié a quitté l'entreprise », indique Romain Caffier. Enfin, lorsque les données sont numérisées, l'entreprise doit se tourner vers une solution de stockage sécurisée et ne pas oublier de les sauvegarder.

• LES DOCUMENTS CIVILS ET COMMERCIAUX

Selon leur nature, la durée de conservation est très variable. Ainsi, si les polices d'assurance doivent être gardées seulement deux ans, les contrats d'acquisition ou de cession de biens immobiliers et fon-

SHUTTERSTOCK - KORN

10 ans

c'est la durée pendant laquelle toutes les pièces comptables doivent être archivées.

ciers doivent l'être trente ans. Pour les contrats commerciaux et les documents bancaires (relevés bancaires, talons de chèques…), le délai est de cinq ans, mais il passe à dix ans pour ceux conclus par voir électronique avec des particuliers et dépassant les 120 euros.

• LES PIÈCES COMPTABLES

Livres et registres comptables, bons de commande et justificatifs de livraison, factures clients et fournisseurs… toutes les pièces comptables doivent être archivées durant dix ans à partir de la clôture de l'exercice.

• LES DONNÉES FISCALES

L'ensemble des documents sur lesquels peuvent s'exercer les droits de communication, d'enquête et de contrôle de l'administration doivent être conservés pendant un délai de six ans, soit à partir de la dernière opération mentionnée sur les livres ou registres, soit à compter de la date à laquelle les documents ou pièces ont été établis. Par exemple, les éléments concernant les revenus de 2016, déclarés en 2017, doivent être consultables jusqu'à fin 2022.

• LES DOCUMENTS CONCERNANT LA SOCIÉTÉ

Leur durée de conservation s'étend de cinq à dix ans. Ainsi, pour les comptes annuels (bilan, compte de résultat, annexe…), elle est de dix ans à partir de la clôture de l'exercice. Les feuilles de présence, les rapports du gérant ou du conseil d'administration ainsi que les rapports des commissaires aux comptes doivent, eux, être conservés sur les trois derniers exercices.

• LES DOCUMENTS RH

Pour les données concernant la gestion du personnel, la durée de conservation va de un à cinq ans. Dans la première catégorie, la comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation. Dans la seconde, les documents concernant les contrats de travail, les salaires, les primes ou encore ce qui concerne les régimes de retraite. ■

Jean-Marc Engelhard

> « Si les contrats conclus dans le cadre d'une relation commerciale doivent être conservés durant cinq ans, les contrats conclus par voie électronique avec des particuliers doivent, eux, l'être pendant dix ans »
>
> ***Romain Caffier, expert-comptable au sein du cabinet 3G Gadras, membre du groupement France Défi***

SYSTÈMES D'ARCHIVAGE ÉLECTRONIQUE : CE QU'IL FAUT SAVOIR

Comme pour les documents papier, les fichiers numériques doivent aussi être archivés. Une démarche facilitée par les systèmes d'archivage électronique (SAE), accessibles même aux plus petites entreprises.

Créer des documents, les modifier, les valider, les partager avant de les archiver… Le cycle de vie des fichiers numériques est identique à celui des documents papiers. Envisager d'utiliser un système d'archivage électronique (SAE) de ses documents implique au préalable de s'être équipé d'un outil de gestion électronique des documents (GED). « L'un ne va pas sans l'autre, souligne Philippe Cohen, expert-comptable et commissaire aux comptes au cabinet Alexma Audit, membre du groupement France Défi. La GED permet de gérer les contenus numériques "vivants", qu'il s'agisse de mails, de factures, de bons de commandes ou de bulletins de paie. Et lorsque ceux-ci n'ont plus d'utilité immédiate, qu'ils sont "figés", ils peuvent basculer dans le SAE afin d'être conservés de manière sécurisée et pérenne. » Une salle d'archivage virtuelle dans laquelle ils resteront le temps nécessaire, notamment en fonction des délais de conservation prévus par la loi. « Si, dans une multinationale, les documents d'importance secondaire ne sont pas conservés, dans une TPE et une PME, il n'est pas nécessaire d'effectuer un tri, car, pour des tarifs très abordables, les capacités de stockage propo-

SHUTTERSTOCK - ONE PHOTO

SAE

Le système d'archivage électronique vient en complément de la gestion électronique des documents.

sées ne cessent d'augmenter », remarque Philippe Cohen. Certaines pièces, elles, devront être mises à l'abri dans un coffre-fort numérique. « C'est le cas des factures électroniques, mais aussi des documents émis dans certains métiers, comme les notaires », précise Philippe Cohen.

SÉCURITÉ GARANTIE CHEZ LES LEADERS DU STOCKAGE

Avant d'opter pour l'un ou l'autre système d'archivage, mieux vaut s'assurer de sa compatibilité avec son outil de GED afin d'automatiser l'archivage. Une possibilité offerte, notamment pour les petites structures, par les leaders mondiaux du stockage et de l'archivage que sont Google, Amazon, Microsoft et Apple. G Suite de Google, par exemple, permet pour des coûts modiques de gérer ses documents dans son Drive puis de les archiver automatiquement. « Cette solution est d'ailleurs compatible avec d'autres GED, qu'il s'agisse de GED "métiers" développées par des éditeurs indépendants et répondant aux besoins de professions spécifiques, ou de GED conçues sur-mesure pour des activités très pointues », constate Philippe Cohen. Avantage : ces géants du numérique bénéficient des technologies les plus avancées en matière de sécurité. Il y a donc peu de risques de voir ses données perdues à cause d'une cyberattaque. ■

Jean-Marc Engelhard

> « Lorsque les documents n'ont plus d'utilité immédiate, qu'ils sont "figés", ils peuvent basculer dans le SAE afin d'être conservés de manière sécurisée et pérenne »
>
> ***Philippe Cohen, expert-comptable et commissaire aux comptes au cabinet Alexma Audit, membre du groupement France Défi***

COLLECTER
HÉBERGER
ARCHIVER
4 SÉCURISER
PRÉVENIR ET ASSURER

CINQ CONSEILS POUR SÉCURISER SES DONNÉES NUMÉRIQUES

Gérer les informations d'une entreprise par la voie électronique présente bien des avantages, mais n'est pas sans risque. L'entreprise dispose néanmoins de moyens faciles à mettre en place pour parer aux principaux dangers.

Mails, factures numériques, plateforme d'échange de documents avec les services de l'État, la dématérialisation fait aujourd'hui partie du quotidien du chef d'entreprise. Une évolution qui n'est pas sans risque. Les données stratégiques de l'entreprise comme celles, personnelles, de son dirigeant peuvent faire l'objet de piratage ou d'intrusion. « L'enjeu pour le chef d'entreprise est donc de prendre des mesures pour se protéger », souligne Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre de France Défi. Des solutions souvent simples et peu coûteuses le permettent.

1. PROTÉGER SON ORDINATEUR ET SES OUTILS

Une première précaution consiste à protéger son ordinateur et ses outils. « Les antivirus et les filtres antihameçonnage, mis à jour, constituent la base de la protection et, dans l'idéal, il faut utiliser un poste différent suivant son usage professionnel ou personnel », conseille Alain Borghesi, président de Cecurity.com (lire article « Cybersécurité : quatre outils pour être bien protégé »).

2. RÉFLÉCHIR À SES MOTS DE PASSE

« Mieux vaut également mettre en place des mots de passe différents et de plus en plus compliqués, pour les utilisations basiques, ce qui touche aux données de l'entreprise, les sites sensibles et ce qui est

SHUTTERSTOCK - ONEPHOTO

8 c'est le nombre minimal de caractères qu'il faut pour créer un bon mot de passe

personnel au chef d'entreprise », estime Pascal Guicherd. Un bon mot de passe contient au moins huit caractères de différents types et évite les informations de base comme des noms ou des dates. Le changer régulièrement et paramétrer ses outils pour limiter le nombre de tentatives de connexions font également partie des bonnes pratiques.

3. METTRE EN PLACE UNE CHARTE INFORMATIQUE

Le chef d'entreprise doit aussi veiller à limiter les failles au sein de l'entreprise. Cela passe notamment par l'information des collaborateurs. « On peut édicter une charte qui explique ce que l'on peut et ne peut pas faire. Je conseille en tout cas de nommer une personne chargée de la sécurité informatique, qui puisse dresser un inventaire des outils, des logiciels, des accès et des problèmes éventuels », suggère Pascal Guicherd. Au-delà des ordinateurs, ce sont tous les objets connectés mais aussi par exemple sa box Internet qu'il faut penser à sécuriser. Mieux vaut également sectoriser les accès : le commercial n'a pas besoin de disposer des informations comptables par exemple.

> « Je conseille en tout cas de nommer une personne chargée de la sécurité informatique, qui puisse dresser un inventaire des outils, logiciels, accès et des problèmes éventuels »
>
> *Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre du groupement France Défi*

4. DISPOSER D'UN COFFRE-FORT ÉLECTRONIQUE

Pour protéger les données les plus stratégiques ou confidentielles, coordonnées bancaires, brevets, contrats ou bilans comptables de l'entreprise, il est enfin possible d'utiliser des solutions sécurisées de stockage en ligne appelées coffres-forts numériques. « L'utilisateur va générer une clé de déchiffrement qui sera nécessaire pour accéder aux fichiers chargés dans le coffre », explique Alain Borghesi, qui propose des coffres-forts labellisés par la Cnil.

5. ASSURER LA NON-MODIFICATION DES DOCUMENTS ARCHIVÉS

Certains services permettent également de garantir la date et la non-modification des documents archivés. Une garantie intéressante s'agissant des pièces que les entreprises ont l'obligation de conserver. « On ne peut pas tout mettre dans un coffre-fort ou dans une solution de sauvegarde externalisée, mais, pour les documents sensibles, c'est la solution la plus efficace et il en existe à des coûts très raisonnables, de l'ordre de 200 à 500 € par an », précise Pascal Guicherd. ■

Marion Perrier

QUELQUES GESTES À RETENIR AU QUOTIDIEN :

- soigner ses mots de passe : 8 caractères de différents types sans information personnelle de base;
- mettre ses logiciels régulièrement à jour : pour se protéger des virus identifiés;
- télécharger les logiciels sur les sites officiels des éditeurs;
- ne jamais ouvrir une pièce jointe d'un mail inconnu.

CYBERSÉCURITÉ : QUATRE OUTILS POUR ÊTRE BIEN PROTÉGÉ

Plus les circuits d'information d'une entreprise font appel au numérique, plus son système informatique doit être sécurisé. Voilà quatre outils et démarches indispensables pour se prémunir des risques d'intrusion, d'altération ou de vol de données.

• CYBERSÉCURITÉ : UN ANTIVIRUS MIS À JOUR

À défaut d'être totalement infaillibles, les antivirus sont indispensables. « Les virus mutent si vite que les outils chargés de les traquer n'ont pas toujours le temps de s'y adapter, mais ils contribuent à renforcer la sécurité », assure Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre du groupement France Défi. Les antivirus préinstallés sur les systèmes d'exploitation récents s'avèrent assez efficaces. Parmi les solutions payantes, Norton, Kaspersky et Bitdefender tiennent la corde. Mais Avast est un très bon choix… gratuit ! Reste ensuite à vérifier régulièrement que ceux-ci sont activés et à jour ! À noter : pour augmenter au maximum les chances de stopper les attaques, il est conseillé d'installer des antivirus différents sur les serveurs et les postes de travail.

SHUTTERSTOCK - BOIKO Y

24 000

cyberattaques ont été déjouées en France en 2016.

Source : Ministère de la Défense, 2016

UN FIREWALL BIEN PARAMÉTRÉ

Contrôlant le trafic et filtrant les flux de données afin de protéger le système des intrusions, un firewall constitue le premier niveau de protection d'un système d'information. « Son paramétrage, souvent complexe, doit être effectué avec soin. Si l'entreprise n'a pas prévu de permettre à ses clients d'accéder à certaines fonctionnalités internes, les accès depuis l'extérieur doivent être fermés », souligne Pascal Guicherd. Dans le cas inverse, les autorisations d'accès doivent être bien délimitées. Enfin, un firewall doit être protégé par un mot de passe robuste, afin d'en rendre l'accès impossible à qui souhaiterait le désactiver.

UN ANTISPAM DE DERNIÈRE GÉNÉRATION

La messagerie électronique, c'est le maillon faible d'un système d'information, par lequel passent la majorité des infections. « Filtrer les e-mails avant même qu'ils arrivent sur le serveur de l'entreprise est donc essentiel. Pour cela, un antispam est de rigueur, et de préférence de dernière génération », prévient Cédric Manca, directeur des centres de services sécurité de l'intégrateur Exaprobe. « Les plus efficaces sont ceux qui demandent une authentification lors d'un premier échange, comme Mail In Black. Ils sont infranchissables par les robots ! » explique Pascal Guicherd. Dans ce domaine, il existe d'ailleurs des solutions externalisées, telles que Altospam, avec mises à jour automatisées. Les mails indésirables sont filtrés sans qu'il soit nécessaire d'installer un logiciel.

DES DONNÉES « SECTORISÉES »

À l'exception de la direction, aucun salarié n'a besoin d'avoir accès à l'ensemble des informations de l'entreprise. « Pour réduire les risques, les entreprises peuvent sectoriser leur système d'information, en ne permettant à leurs collaborateurs d'accéder qu'aux données dont ils ont besoin dans le cadre de leur activité », explique Cédric Manca. Une « gestion des identités » qui s'apparente aux habilitations données à chaque intervenant dans des secteurs sensibles comme la défense. À ne pas négliger enfin, l'obligation faite aux salariés d'adopter des mots de passe robustes. En fonction de leur niveau de complexité, il faut entre quelques minutes et plusieurs dizaines d'années aux robots malveillants pour les « cracker » ! ■

Jean-Marc Engelhard

> « Pour réduire les risques, les entreprises peuvent sectoriser leur système d'information, en ne permettant à leurs collaborateurs d'accéder qu'aux données dont ils ont besoin dans le cadre de leur activité »
>
> ***Cédric Manca, directeur des centres de services sécurité de l'intégrateur Exaprobe***

ENTREPRISES : OÙ METTRE VOS DONNÉES À L'ABRI ?

Effectuer la sauvegarde de ses données ? Confier cette tâche à une société spécialisée ? Dans tous les cas, mieux vaut être prévoyant et ne pas s'en remettre à un simple disque dur externe.

Sauvegarder n'est pas archiver ! Ce qui les distingue ? À la différence d'un simple moyen de stockage, une solution de sauvegarde doit permettre de restaurer l'ensemble d'un système, logiciels compris, en cas de sinistre matériel ou d'acte malveillant. « Des accidents qui n'arrivent pas qu'aux autres ! », rappelle Stéphane Sécher, du cabinet Abaq Conseil et Expertise comptable, membre du groupement France Défi.

SE MÉFIER DES SOLUTIONS BASIQUES

Afin de mettre à l'abri leurs données, plusieurs options s'offrent aux entreprises. Pour les plus petites, c'est souvent la sauvegarde régulière des données sur un disque dur externe ou une clé USB qui est retenue. « Attention, prévient Stéphane Sécher, ces outils sont une cible facile pour les virus et les ransomware. Lorsque l'on s'aperçoit de leurs méfaits sur un système d'information, le plus souvent, ils se sont déjà infiltrés sur le disque dur externe ou la clé USB. » Autrement dit, ces supports sont loin d'être infaillibles. Autre option, l'externa-

SHUTTERSTOCK - DEN RISE

68 %

des sociétés suivies par l'Observatoire épargnées grâce aux sauvegardes.

Source : Observatoire de la cyberprévention France Défi

lisation de la sauvegarde. « Lorsque l'on fait appel à une société de services informatiques pour gérer son système d'information, il est préférable de lui demander conseil pour déterminer la solution la plus adaptée », préconise Stéphane Sécher. Un impératif : que l'option retenue sauvegarde tout l'environnement de travail, données mais aussi système d'exploitation et logiciels, afin de permettre une restauration complète. Avant de s'engager, il est indispensable de se pencher sur le délai de récupération des données, qui peut varier. Idem pour la récurrence des sauvegardes. « Pour certaines entreprises, la perte d'une journée d'activité n'est pas dramatique tandis que, pour d'autres, une sauvegarde effectuée plusieurs fois par jour est indispensable », note Stéphane Sécher. Une décision à prendre en fonction du rapport risques/coûts. Certains éditeurs proposent des solutions de sauvegarde adaptées aux petites entreprises.

> « Pour certaines entreprises, la perte d'une journée d'activité n'est pas dramatique tandis que, pour d'autres, une sauvegarde effectuée plusieurs fois par jour est indispensable »
>
> *Stéphane Sécher, cabinet Abaq Conseil et Expertise comptable, membre du groupement France Défi*

LES ATOUTS DES SERVEURS VIRTUALISÉS

Autre alternative, la sauvegarde des données sur un serveur installé dans les locaux de l'entreprise. Une option qui vaut uniquement pour celles qui disposent d'une expertise informatique en interne. Certains prestataires proposent des serveurs virtualisés. Le principe ? Une seule machine physique permet de faire fonctionner plusieurs serveurs virtuels, ce qui a pour conséquence une simplification de l'installation et une limitation des coûts liés au matériel et à son exploitation ainsi qu'à la consommation d'énergie. Quelle que soit la solution technique, la seule garantie de son efficacité reste la réalisation d'un crash test. « Celui-ci peut n'être effectué que sur quelques données précises, afin de vérifier que leur restauration ne pose pas de problème », précise Stéphane Sécher. Pas question en effet de prendre le risque de perdre l'ensemble de ses données si le système ne répond pas aussi bien que prévu ! ■

Jean-Marc Engelhard

UN COFFRE-FORT POUR STOCKER SES DOCUMENTS NUMÉRIQUES

Utile pour entreposer des documents importants, un coffre-fort numérique offre bien d'autres avantages. Zoom sur les atouts de ce nouvel outil d'archivage.

Certains utilisent des solutions de cloud ou de gestion électronique des documents (GED) pour conserver leurs fichiers numériques. D'autres préfèrent les entreposer dans un coffre-fort électronique. «Ce sont des solutions de stockage qui n'ont pas le même degré de sécurisation. Seuls les coffres-forts électroniques possèdent des normes de sécurité proches de celles du domaine bancaire», note Pascal Guicherd, responsable de MG Systèmes d'information, une filiale du cabinet d'expertise comptable rhônalpin MG, membre du groupement France Défi, spécialisée dans l'installation et la maintenance de postes de travail et de logiciels.

UN OUTIL UTILE AUX DIRIGEANTS D'ENTREPRISE

Cette sécurité se manifeste notamment par le fait que les documents qu'il contient sont cryptés dès leur envoi et le restent même lorsqu'ils sont consultés. «A priori, un coffre-fort électronique est personnel, mais il est possible d'en partager l'accès entre les deux ou trois cadres dirigeants d'une même entreprise. Il permet de centraliser des dossiers clés et de les consulter sans danger de n'importe quel ordinateur», souligne Pascal Guicherd. Il est d'ailleurs envisageable de partager pendant une durée limitée un contrat ou un plan de financement avec un tiers qui pourra seulement le consulter. Autre atout de cet outil, la possibilité de le paramétrer afin qu'il aille directement «aspirer» ses factures sur le site de son opérateur téléphonique ou ses déclarations auprès des impôts. «La recherche est d'autant plus simple que les fichiers peuvent être tagués avec des mots

ISTOCK - PETAR CHERNAEV

Intégrité

Un document conservé dans un coffre-fort électronique ne peut être modifié.

clés», précise Pascal Guicherd. Dernier avantage, et pas des moindres pour les chefs d'entreprise : le téléchargement dans un coffre confère une date probante aux documents, et leur apporte ainsi une sécurité juridique.

CHOISIR LE BON PRESTATAIRE

De nombreuses sociétés proposent des coffres-forts électroniques. Mais, avant de s'engager, mieux vaut vérifier le sérieux du prestataire, par exemple en s'assurant qu'il dispose du label de la Fédération nationale des tiers de confiance (FNTC). Autre sujet d'interrogation, la pérennité de ce fournisseur. «Qu'advient-il des documents que l'on a stockés depuis des années si celui-ci disparaît ?», s'interroge Pascal Guicherd. Par prudence, il est préférable de se tourner vers une entreprise solide, voire dépendant de l'État, comme Digiposte, de La Poste, ou une solution proposée par les banques ou les compagnies d'assurances.

PROPOSER UN COFFRE-FORT ÉLECTRONIQUE À SES SALARIÉS

Au sein du cabinet d'expertise comptable rhônalpin MG, chaque collaborateur bénéficie d'un coffre-fort électronique. «C'est dans ce coffre que nous leur envoyons leurs bulletins de paie. Ils peuvent également l'utiliser pour centraliser des documents administratifs, des factures ou encore des copies de leurs papiers et de leur permis de conduire», précise Pascal Guicherd. Le tout gratuitement pour les particuliers jusqu'à environ 5 Go. Quant aux solutions d'entreprises, elles sont très accessibles. Pour une petite structure, le tarif d'un coffre-fort de 15 Go accessible à cinq utilisateurs ne dépasse pas 50 € HT par mois. ■

Jean-Marc Engelhard

QUATRE SOLUTIONS POUR LES PME ET LES INDÉPENDANTS

E-COFFREFORT.FR : Cette solution a été créée en 2006 par l'Office français pour la sécurité et l'archivage des documents (OFSAD), membre de la FNTC (Fédération nationale des tiers de confiance). L'OFSAD s'engage notamment à restituer des copies de tous les documents d'origine plus de trente ans après leur dépôt.

XAMBOX : Adaptée à l'activité des professionnels indépendants, Xambox permet de retrouver facilement les fichiers conservés dans un coffre-fort numérique sécurisé, grâce à un moteur de recherche avancé et à une reconnaissance optique des caractères dans les documents.

CECURCRYPT BUSINESS : Cette solution est développée par Cecurity.com, un éditeur de logiciels d'échanges sécurisés et d'archivage des originaux numériques. C'est la première entreprise à avoir obtenu le label Coffre-Fort numérique de la Cnil.

VAULT : C'est la partie coffre-fort numérique de G Suite, la solution de Google proposée aux entreprises, intégrant notamment Google Drive, qui permet de stocker, synchroniser et partager des fichiers.

DEUX SOLUTIONS POUR LES SALARIÉS

DIGIPOSTE : Lancé en 2011 par La Poste, Digiposte permet de sauvegarder gratuitement jusqu'à 5 Go. Récemment, La Poste a lancé l'appli Digiposte +, qui récupère et organise automatiquement factures et relevés de plus de 300 organismes (impots.gouv.fr, La Banque Postale, BNP Paribas, Uber, EDF, Orange…).

MYPEOPLEDOC : Accessible aux salariés gratuitement et à vie (même s'ils changent d'entreprise), ce coffre-fort électronique permet aux employeurs de transmettre au personnel l'ensemble des documents RH, comme les feuilles de paie électronique.

COLLECTER
HÉBERGER
ARCHIVER
SÉCURISER

5 PRÉVENIR ET ASSURER

CYBERPRUDENCE : COMMENT SENSIBILISER SON PERSONNEL ?

Tous les salariés n'ont pas intégré les risques induits par l'explosion de la cybercriminalité. Des sessions d'information, de formation et de communication ciblées sur les nouvelles pratiques des cybercriminels peuvent contribuer à accélérer la prise de conscience.

Plus aucune entreprise, quelle que soit sa taille, n'est à l'abri d'une attaque de cybercriminels. C'est une réalité dont tous les salariés n'ont pas encore pris conscience. « Pour en souligner l'importance, la question doit être portée par la direction générale », conseille Coralie Héritier, directrice générale d'IDnomic, éditeur de logiciels spécialisé dans la sécurisation des données et de l'identité numérique. Elle doit par ailleurs être abordée d'entrée de jeu avec les nouveaux collaborateurs. « Lorsque l'entreprise dispose d'une charte informatique, ce qui est fortement recommandé, celle-ci doit être annexée au règlement intérieur, remise avec le livret d'accueil et signée lors de l'entrée en fonction pour en confirmer la prise de connaissance », poursuit Coralie Héritier. Ce document peut d'ailleurs prévoir des sanctions disciplinaires, mais aussi rappeler les risques de poursuites judiciaires, par exemple en cas de violation des droits d'auteur.

CYBERPRUDENCE : UNE ALERTE SUR LES NOUVEAUX RISQUES

Au-delà de ces précautions formelles, une sensibilisation aux bonnes pratiques est indispensable. « Celle-ci doit être pragmatique et s'appuyer sur des exemples concrets », explique Michel Guillout, responsable informatique et qualité de Cigeco. Ce cabinet d'expertise comptable, membre de France Défi, a mis en place des sessions

SHUTTERSTOCK - RAWPIXEL.COM

65%

des attaques par mail réussissent suite à la négligence d'un collaborateur.

Source : Observatoire de la cyberprévention France Défi

d'une demi-journée de formation à la sécurité informatique dans le cadre de son dispositif d'intégration des nouveaux collaborateurs. « Il existe de nombreux outils disponibles en ligne qui peuvent servir de support, comme les guides de bonnes pratiques proposés par l'Agence nationale de sécurité des systèmes d'information (Anssi) ou le site Hack Academy, développé notamment par le Club informatique des grandes entreprises françaises (Cigref) pour alerter, sur un ton décalé, sur les cyberrisques », remarque de son côté Coralie Héritier. Pour éviter que cette préoccupation passe au second plan, rien ne vaut des piqûres de rappel régulières. « Par mail ou sur l'intranet, nous rappelons régulièrement les principaux risques et les manières de s'en prémunir. Et nous envoyons des alertes lorsque de nouveaux types de pratiques frauduleuses apparaissent afin de favoriser la prudence », indique Michel Guillout.

DES RÈGLES À DÉFINIR EN FONCTION DE SON ACTIVITÉ

Principal point d'entrée des virus et des ransomware, la gestion des messageries électroniques doit être au cœur de la prévention. Dans ce domaine, les règles doivent être claires. Les mots de passe doivent être robustes, c'est à dire comprendre des caractères alphanumériques et spéciaux. Ils doivent également être régulièrement modifiés. « Au sein de notre cabinet, les collaborateurs sont contraints de le faire tous les 46 jours », indique Michel Guillout. D'autres sujets doivent aussi faire l'objet de mises en garde, comme l'obligation de passer les fichiers extérieurs à l'antivirus avant de les introduire dans le système d'information de la société ou l'interdiction d'y connecter des clés USB venues de l'extérieur. À chaque entreprise, ensuite, de définir des règles et de les rappeler en fonction de son activité et des contraintes de ses salariés. ■

Jean-Marc Engelhard

> « Lorsque l'entreprise dispose d'une charte informatique, ce qui est fortement recommandé, celle-ci doit être annexée au règlement intérieur, remise avec le livret d'accueil et signée lors de l'entrée en fonction »
>
> ***Coralie Héritier, directrice générale d'IDnomic***

PENSEZ À METTRE EN PLACE UNE CHARTE INFORMATIQUE

Fixer des règles claires, tracer une frontière entre ce qui est autorisé et ce qui ne l'est pas, se protéger de l'intrusion de cybercriminels, informer les salariés des modalités de contrôle de leur employeur… Autant de sujets qu'il est utile d'aborder dans une charte informatique.

De plus en plus d'entreprises se dotent d'une charte de sécurité informatique. Une nécessité pour établir des règles claires d'utilisation du système d'information et se prémunir contre les attaques des cybercriminels. Une fois rédigé, ce document doit être porté à la connaissance du personnel par tous les moyens. « Il peut être affiché, transmis avec la première feuille de paie ou validé par chaque salarié lors de sa première connexion à son poste de travail », explique Pascal Guicherd, directeur informatique du cabinet d'expertise comptable MG, membre du groupement France Défi. Pour être exécutoire, la charte doit être déposée au greffe du tribunal des prud'hommes et transmise à l'inspection du travail. Dans tous les cas, elle doit faire l'objet d'un toilettage régulier, au maximum tous les cinq ans, pour s'adapter à l'évolution des technologies.

CE QUI EST AUTORISÉ

Et le contenu ? Il doit balayer l'ensemble des sujets en lien avec le système d'information, y compris la téléphonie mobile et fixe. « En préambule, cette charte doit préciser les modalités de connexion

SHUTTERSTOCK - RAWPIXEL.COM

61 %

des employés en France utilisent un ordinateur en 2016.

Source : Eurostat, enquête communautaire sur l'usage des TIC et le commerce électronique

au système d'information de l'entreprise, en rappelant notamment le niveau de complexité des mots de passe et la périodicité de leur renouvellement », note Pascal Guicherd. Elle doit aussi rappeler l'interdiction de désactiver les antivirus, la marche à suivre en matière d'utilisation des programmes et des fichiers, et préciser le format et le contenu des fichiers qu'il est possible d'envoyer ou d'ouvrir. « C'est aussi l'occasion de rappeler l'interdiction de télécharger des logiciels sans l'accord du service informatique ou de brancher une clé USB personnelle. Idem pour l'utilisation du poste de travail à des fins répréhensibles comme le téléchargement illégal », relève encore Pascal Guicherd. Internet constitue l'un des principaux sujets abordés dans la charte : certaines entreprises le limitent à un usage strictement professionnel, d'autres font preuve de davantage de souplesse et permettent à leur personnel de consulter messageries personnelles et réseaux sociaux, pour autant qu'il n'y ait pas d'abus.

Pour être exécutoire, la charte doit être déposée au greffe du tribunal des prud'hommes et transmise à l'inspection du travail

ENCADRER L'USAGE DES SMARTPHONES ET LE BYOD

Autre sujet abordé : le contrôle des données par l'entreprise. Il peut, par exemple, être spécifié que l'employeur a la possibilité de consulter les mails de ses salariés, notamment en cas d'absence, à l'exception de ceux dont l'objet mentionne expressément le terme « personnel ». « Dès lors que des contrôles sont envisagés, le traitement mis en œuvre doit être déclaré à la Commission nationale de l'informatique et des libertés (Cnil) », prévient Pascal Guicherd. La charte doit aussi encadrer l'usage des smartphones, puisqu'ils proposent les mêmes fonctionnalités que les ordinateurs, et le Byod (pour « bring your own device », soit le matériel informatique personnel utilisé par le salarié au travail). Les salariés ont-ils le droit d'utiliser leur propre matériel pour se connecter au bureau ? Peuvent-ils utiliser le matériel professionnel à leur domicile, le prêter à leurs enfants ? Si oui, à quelles conditions ? À chaque entreprise de répondre à ces questions. Toutes ces dispositions peuvent donner lieu à des sanctions, qui peuvent elles aussi être énumérées précisément dans la charte. ■

Jean-Marc Engelhard

CYBERCRIMINALITÉ : COMMENT ÉCHAPPER AU RANÇONNING ?

Prendre en otage les données informatiques d'une entreprise est une pratique de plus en plus répandue chez les cybercriminels. Quelques précautions pour ne pas tomber dans leurs filets.

« C'est au retour des vacances de Noël que nous nous sommes aperçus que certains fichiers étaient cryptés et donc inaccessibles. Un message indiquait qu'il fallait payer 250 € pour pouvoir y accéder à nouveau, raconte Philippe Guermeur, associé dirigeant du cabinet d'expertise comptable 3G-Gadras situé à Artigues-près-Bordeaux (33) et président du groupement France Défi. Heureusement, cette tentative survenait après une période de fermeture et, de plus, nous réalisons des sauvegardes quotidiennes. L'activité a donc rapidement pu reprendre. » Le rançonning ou « ransomware », autrement dit le cryptage de toutes les données d'une entreprise, « libérables » après versement d'une rançon, est une mésaventure de plus en plus courante, qui touche des entreprises de toutes tailles. « Pas une semaine sans qu'un client nous appelle pour nous faire part d'une telle cyberattaque. Les organisations qui les lancent sont désormais passées à un stade industriel, aucune entreprise n'est à l'abri, même pas les plus petites, qui pensent souvent ne pas pouvoir être ciblées », remarque Pascal Guicherd, responsable de MG Systèmes d'information, une filiale du cabinet d'expertise comptable rhônalpin MG, membre de France Défi, spécialisée dans l'installation et la maintenance de postes de travail et de logiciels. Le virus WannaCry, en mai 2017, en est un exemple édifiant : en quelques jours,

SHUTTERSTOCK - GUALTIERO BOFFI

1007 $

demandés en rançon en 2016 en moyenne, contre 373 $ en 2014.

Source : Heise de Symantcec, Journal du net Statista

plusieurs centaines de milliers d'entreprises dans plus de 150 pays ont été touchées.

DES ANTIVIRUS LOIN D'ÊTRE INFAILLIBLES

La nature des attaques changeant en permanence, les antivirus sont loin de constituer un rempart infranchissable pour le rançonning. « La première des précautions est technique, elle consiste à privilégier des systèmes d'exploitation récents, et régulièrement mis à jour, mieux armés pour résister aux actions malveillantes. Par ailleurs, il est préférable de mettre en place des antivirus de marques différentes sur les postes de travail et sur le serveur », recommande Pascal Guicherd. En espérant que l'un des deux détecte la tentative d'intrusion… Autre mesure préventive, la mise en place d'un plan de sauvegardes des données. « Nous effectuons trois types de sauvegarde, l'une quotidienne, l'autre mensuelle et la dernière annuelle », explique ainsi Philippe Guermeur. « Lorsque c'est une sauvegarde "maison", le support la contenant ne doit pas être conservé dans l'entreprise, précise Pascal Guicherd. Il existe aussi des services de sauvegarde externalisés via Internet, dont le coût est raisonnable, certaines s'effectuant même en temps réel. »

FACE AU RANÇONNING, UNE SENSIBILISATION DES SALARIÉS INDISPENSABLE

Toutes ces précautions ne doivent pas faire oublier que ce sont les utilisateurs eux-mêmes, autrement dit les salariés, qui font entrer le loup dans la bergerie. « La grande majorité des virus s'introduisent par le biais des messageries électroniques. Il n'est pas inutile de rappeler qu'il ne faut pas ouvrir les pièces jointes des mails suspects, en particulier ceux qui arrivent sans texte dans le corps du message, même si l'adresse de l'expéditeur est connue », souligne Pascal Guicherd. Tout aussi risqué : la visite de sites non fiables, voire douteux, le téléchargement de logiciels sans autorisation préalable du responsable informatique ou encore l'utilisation de clés USB n'ayant pas été fournies par l'entreprise. Autant de précautions à rassembler au sein d'une charte des bonnes pratiques informatiques et devant régulièrement faire l'objet de piqûres de rappel. Dernière possibilité : prendre une assurance contre le risque informatique. Cette option est loin d'être accessoire, car l'indisponibilité d'un système d'information ou la perte de données peuvent avoir des conséquences désastreuses sur l'activité, coûter cher en termes d'image, voire, dans des cas extrêmes, se solder par la fermeture de l'entreprise. ■

Jean-Marc Engelhard

EN SAVOIR PLUS

- Des informations sur la cybercriminalité et des recommandations pratiques pour s'en protéger sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : www.ssi.gouv.fr
- Des informations sur la cybercriminalité et des conseils techniques sur le site du Club de la sécurité de l'information français (CLUSIF) : https://clusif.fr

S'ASSURER CONTRE LA CYBERCRIMINALITÉ

Il est devenu impossible, aujourd'hui, de se passer des réseaux Internet et de leurs opportunités commerciales. Pourtant la fluidité des échanges peut se retourner contre l'entreprise quand des individus parviennent à pénétrer son système informatique.

En décembre 2015, le fabricant de jouets asiatique VTech avouait s'être fait pirater près de 5 millions de comptes clients du monde entier, dont environ 900 000 en France. Un peu avant, en avril 2015, la chaîne internationale francophone TV5Monde, diffusée dans 200 pays, subissait une cyberattaque massive de pirates qui interrompait la totalité de ses programmes pendant huit heures. Ces attaques peuvent coûter très cher : TV5Monde devrait dépenser une douzaine de millions d'euros au total d'ici à 2018, rien qu'en réparations informatiques. On comprend dès lors l'intérêt de souscrire une assurance contre les conséquences du cybercrime.

CYBERCRIME : 3 FORMES PRINCIPALES

Au cabinet d'experts-comptables Cigeco, membre du groupement France Défi, à Limoges (Haute-Vienne), Michel Guillout, directeur informatique, distingue trois formes principales de cybercrime. La première ? Rendre indisponibles les données « quand quelqu'un bloque votre activité. Si vous avez un site de e-commerce, vos

SHUTTERSTOCK - BRIAN A JACKSO

1/4

des attaques ciblées ont abouti à une violation effective des dispositifs de sécurité en 2016 en France.

Source : étude Accenture, 2016

ventes chutent. Et si on vous injecte un virus, cela peut bloquer tout votre système informatique ». Deuxième forme courante de cybercrime : le vol de données de l'entreprise, « très gênant en termes de responsabilité et d'image » vis- à-vis des clients et du marché. La troisième forme d'attaque, la plus courante, l'extorsion ou rançonning, survient « lorsque quelqu'un parvient à crypter vos données et vous demande une rançon pour les décrypter », achève Michel Guillout.

QUELLES GARANTIES ?

Aujourd'hui, la plupart des assureurs proposent des garanties contre ces trois formes de cybercriminalité. Au minimum, l'assurance en responsabilité civile, qui permet d'indemniser les tiers (clients, fournisseurs) en cas de dommage, est généralement étendue aux cyberrisques. Selon les formules, les assureurs peuvent aussi aller plus loin et prendre en charge les pertes d'exploitation de l'entreprise, ou encore les frais de notification, comme Generali dans sa nouvelle offre Generali Protection numérique. Il est en effet obligatoire d'avertir la Cnil et les clients en cas de cyberattaque.

Une nouvelle réglementation européenne entrera en vigueur le 25 mai 2018 et porte notamment sur une nouvelle « obligation de notification ». Le « Règlement général sur la protection des données » (RGPD) deviendra la référence en matière de protection des données à caractère personnel au sein de l'Union européenne. Conséquence pratique pour les entreprises : l'obligation de notifier les failles de sécurité s'applique à tous les responsables de traitement de données ainsi qu'aux sous-traitants. Suivant la gravité de la situation, la communication de la faille de sécurité pourra s'étendre à l'ensemble des personnes éventuellement concernées, fournisseurs comme clients…

ATTENTION AUX EXCLUSIONS

Chez Axa, les trois niveaux d'assurance (RC, pertes d'exploitation, frais de communication) sont proposés. Chez tous les assureurs, les tarifs se négocient et varient en fonction des risques couverts et de la taille de l'entreprise. Les primes d'assurance démarrent entre 1 500 € et 2 500 € annuels pour des montants de garantie de 250 000 à 700 000 €. Certains assureurs, comme Allianz, garantissent jusqu'à 20 à 30 millions d'euros. « Si l'entreprise est très prudente et a assuré des sauvegardes, elle peut se permettre de prendre une prime assez faible », estime cependant Michel Guillout. Comme pour toute assurance, il faut prendre garde aux franchises – les montants qui resteront à votre charge –, et aux clauses d'exclusion : « Certaines assurances ne vous couvrent plus si une faute a été commise au niveau de l'entreprise », avertit Michel Guillout.

ANTICIPER LES RISQUES

« Avant de souscrire une telle assurance, il est nécessaire de cartographier ses risques et de mettre en place les systèmes de sécurité adéquats », estime Michel Guillout. Une petite entreprise dans les biotechnologies sera une cible hautement stratégique. Les cabinets d'experts-comptables, les journalistes et les avocats aussi… Mais bien d'autres activités peuvent être victimes de cyberattaques. « Un de mes clients, un hôtelier, s'était fait crypter ses fichiers clients. Les pirates lui demandaient 900 dollars. Heureusement il avait assez de sauvegardes pour n'avoir pas à payer la rançon », se souvient

> « Avant de souscrire une telle assurance, il est nécessaire de cartographier ses risques et de mettre en place les systèmes de sécurité adéquats »
>
> *Michel Guillout, directeur informatique de Cigeco, membre du groupement France Défi*

Michel Guillout. Former les salariés à la sécurité informatique et mettre en place des techniques de sécurisation des données sont aujourd'hui incontournables. « Il faut également penser au plan de reprise d'activité (PRA) après l'attaque », souligne Michel Guillout. L'assurance est ce qui vient en plus, lorsque tout le reste a déjà été envisagé. ■

Anne-Claire Ordas

« ENCORE UN MARCHÉ DE NICHE »

Malgré les récents piratages qui ont fait l'actualité, les professionnels de l'assurance observent que les sollicitations des entreprises sur la question demeurent encore faibles. « Il n'y a pas d'augmentation spectaculaire des demandes et c'est assez logique car les offres sur le marché sont encore limitées », explique Frédéric Lassureur, expert indépendant, intervenant dans le secteur depuis trente ans. Il précise que les professionnels intéressés par une couverture supplémentaire d'un risque lié à la cybercriminalité ne la trouveront pas toujours chez leur assureur. « C'est une tendance, mais en aucun cas un marché en pleine expansion. Pour l'instant, les offres d'acteurs comme Axa, Hiscox ou Zurich Insurance sortent du lot sur le marché mais c'est encore un marché de niche. » Axa propose par exemple, après diagnostic de l'entreprise, une réponse assurantielle complète (vol de données clients, pertes d'exploitation, atteinte à l'e-réputation) avec une aide à la prévention et, parmi ses garanties, la reconstitution des données perdues et la couverture des pertes d'exploitation. Quant au contrat Cyber & Data by Hiscox, il promet une protection contre les risques liés à l'exposition des données sensibles. Actualité et risques accrus obligent, l'assureur italien Generali a lancé à son tour cette année une offre incluant assistance, réparation et indemnisation, Generali Protection numérique (GPN), conçue plus particulièrement à destination des TPE et PME exposées aux cyberrisques.

« Pour l'instant, cependant, il n'y a pas assez de demandes pour mutualiser les chaînes nécessaires d'experts spécialistes, tempère Frédéric Lassureur. Pour beaucoup d'acteurs se pose encore la question du prix d'une telle protection et des garanties proposées sachant que le coût pour un client peut varier de un à dix selon la nature des données perdues. » En attendant, néanmoins, beaucoup d'entreprises se reposeront sur leur police existante. « Ces contrats comprennent déjà certaines garanties concernant la perte de matériel informatique dans un incendie, un dégât des eaux ou en cas de vol physique. En même temps, beaucoup de ces garanties reposent aussi sur des procédures hebdomadaires de sauvegarde des données et des mises à jour des logiciels, qui constituent une protection élémentaire. La première assurance est d'avoir au sein de l'entreprise une véritable politique de protection des données. »

Céline Chaudeau

> *« La première assurance est d'avoir au sein de l'entreprise une véritable politique de protection des données »*
>
> ***Frédéric Lassureur, expert indépendant***

TRANSITION DIGITALE : QUELS CHANGEMENTS POUR DEMAIN ?

Et si la transition digitale n'en était qu'à ses débuts ? Régulièrement, des technologies de rupture apparaissent, qui pourraient bien, demain, venir bouleverser les circuits de circulation de l'information et les manières de travailler. À l'image de la blockchain.

Factures et feuilles de paie électroniques, gestion électronique des documents, systèmes d'archivage électronique… Depuis quelques années, le développement du numérique remet régulièrement en question les modes de fonctionnement des entreprises. Quel que soit le secteur d'activité, l'agilité est désormais de mise à tous les étages. Canaux de communication, modes de fabrication, gestion de la relation client, modalités d'échange de l'information… Sur tous ces sujets, les remises en cause sont permanentes. Et c'est sans doute loin d'être fini ! Dans les années qui viennent, d'autres innovations pourraient encore venir modifier les habitudes. À l'image des fameux bitcoins, la monnaie électronique apparue en 2009. Indépendante (car non contrôlée par une institution ou un État), universelle, échangeable en peer-to-peer (directement entre individus, sans passer par une banque), transparente (puisque tous les utilisateurs peuvent accéder aux transactions sur le réseau Bitcoin)… Certains imaginaient cette monnaie numérique faire vaciller le pouvoir des banques. On en est encore loin.

DES MODÈLES ÉCONOMIQUES SOUMIS À LA TECHNOLOGIE

La blockchain, la technologie sur laquelle repose le bitcoin, s'avère, elle, plus prometteuse. Son principe ? « Une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne », selon la définition de la société Blockchain France. Une sorte de grand livre comptable public, anonyme et quasiment impossible à pirater, susceptible de faire office de tiers de confiance. Et qui pourrait bien finir par remplacer ceux auxquels on se fie aujourd'hui, comme les notaires ou les banquiers. Bien d'autres secteurs pourraient être impactés, comme les assurances, l'immobilier ou l'énergie. Certains prédisent même que, grâce à la blockchain, les sociétés de VTC pourraient être remplacées par des plateformes ouvertes où chauffeurs et clients pourront être mis en relation, sans intermédiaire… À peine apparus, les géants de l'économie dite « collaborative » pourraient donc déjà être en danger de disparition ! Là encore, ce n'est pas pour demain, mais peut-être pour après-demain. Cet exemple illustre l'accélération des cycles et l'incidence grandissante de l'innovation technologique sur les modèles économiques. Il rappelle aussi aux chefs d'entreprise que, plus que jamais, la veille technologique est un impératif. ■

POUR EN SAVOIR PLUS CONTACTEZ VOTRE EXPERT-COMPTABLE

CANOPÉECONSULTING
Expertise comptable & conseil

&

rendez-vous sur le site d'information
www.experts-et-decideurs.fr

Édition France Défi - Conception et réalisation : Accroche-com'
Suivi éditorial : Accroche-press' - 2017