

Le Cabinet ACDL Expertise vous informe :

## Transition digitale : votre entreprise est-elle prête ?



**À l'occasion du salon VivaTechnology, Experts & décideurs publie un nouveau dossier thématique téléchargeable en version PDF, qui regroupe un ensemble d'articles du site destinés aux entreprises souhaitant réussir leur transformation numérique.**

Même si toutes les entreprises n'en ont pas encore pris la pleine mesure, la transition numérique est lancée et rien ne l'arrêtera. Au-delà des obligations légales de s'y adapter, cette révolution est source d'opportunités, mais demande quelques efforts ...

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, etc. Autant de nouveautés qui vont permettre à l'entreprise de s'organiser, de se développer, d'anticiper et de mieux maîtriser son activité.

Les changements sont nombreux et bénéfiques, à condition de mettre en place en parallèle de bonnes pratiques. En termes de méthode de travail mais également de process et de mesures de sécurité.

### La digitalisation, oui. La cybercriminalité, non

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.

## L'Observatoire de la cyberprévention France Défi

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 totalise 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.

Ce diagnostic permet à l'Observatoire d'édicter de grands principes à respecter. En premier lieu, établir obligatoirement un plan de sauvegarde l'enquête révèle que : pour 68 % des sociétés, les menaces ont été déjouées notamment grâce à la restauration de ces sauvegardes.

D'autres précautions sont nécessaires comme l'adoption de mots de passe robustes, d'un antivirus, d'un firewall à jour et d'un antisipam. 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.

Par Accroche-press' pour France Défi  
vendredi 16 juin 2017 15h36

**Les collaborateurs du cabinet se tiennent à votre disposition pour tout renseignement complémentaire.**

Votre expert-comptable : Guillaume GAHIDE 03.27.62.18.11 / ggahide@acdl.fr