Le Gepa crée son Digital Club en pays d'Aix

le 14 septembre 2015 - Martine Debette - Entreprendre - article lu 1 fois

Le groupement des entrepreneurs du Pays d'Aix (Gepa) lance le Digital Club pour créer une dynamique autour des questions numériques.

L'objectif du Digital Club du Gepa du pays d'Aix est de « *sensibiliser les chefs d'entreprises au cours d'un échange convivial et permettre aux acteurs du numérique de se rencontrer et éventuellement de faire du business ensemble* », a indiqué Pascal Tanguy, co-président de la commission Digital Club.

Quatre dîners-conférences seront proposées chaque année sur le thème du numérique. La première rencontre concernait la sécurité dans l'univers numérique. Ely de Travieso, président du Club de la sécurité des systèmes d'information régional (Clusir) Paca, a fait un tour d'horizon des obligations légales du chef d'entreprise qui peut se retrouver en prison à cause d'un site internet, d'un réseau informatique ou d'un poste nomade. A l'heure où les nouvelles technologies sont omniprésentes et où tout le monde ou presque y a accès, la sécurité est de mise. D'autant que la loi indique clairement que « *le responsable du traitement de données à caractère personnel est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données* ».

Préserver la sécurité des données

Car les menaces sont bien réelles. Les *hackers* ne manquent pas d'idées pour s'infiltrer dans les réseaux. Certaines affaires ont d'ailleurs été largement médiatisées. Que l'entreprise soit petite ou grande, les brevets et autres technicités attirent les convoitises. Les techniques des pirates de l'informatique sont diverses, elles vont de l'intrusion informatique, à l'usurpation d'identité en passant par la transmission de virus. Du coup, l'entreprise peut y perdre beaucoup aussi bien financièrement que commercialement, sans oublier les risques liés à la réputation.

Accepter le risque et se protéger

Pour Ely de Travieso :

> ***« [il faut] savoir accepter que le risque ne puisse être protégé à 100% et se déresponsabiliser des risques légaux ».***

Des moyens de protection existent et ils peuvent avoir un coût. C'est le cas de la politique de sécurité des services d'information (PSSI), de l'audit, d'un contrat garantissant un niveau de sécurité, de l'authentification par un « vrai » mot de passe difficile à

trouver pour décourager les éventuels *hacker*s, et ne pas oublier de sauvegarder ses données que des logiciels intrusifs peuvent crypter et rendre inaccessible à moins de payer une rançon pour les récupérer.

Assurances et choix de cloud

D'autres solutions ont fait leur apparition, comme les assurances, le choix du *cloud* par des prestataires qui s'engagent à protéger les données, l'audit inversé avec rémunération de « gentils » *hackers* rémunérés lorsqu'ils trouvent des failles. Enfin, il faut faire preuve de bon sens en sécurisant l'accès wifi de l'entreprise, en bloquant le clavier de son *smartphone* ou de sa tablette avec un code d'accès, en n'insérant pas sa clé USB dans un appareil qui pourrait être infecté, et en séparant les usages personnels des usages professionnels.