La Provence .com

LES ENTREPRISES DU PAYS D'AIX ONT LEUR DIGITAL CLUB

Jeudi 17/09/2015 à 09H30 Aix-en-Provence Tags : Digital club Entreprises Numérique Réagir

L'objectif de cette commission, lancée par le Gepa, est de sensibiliser les patrons à l'univers du numérique, par le biais de conférences

Ely de Travieso, président du Clusir Paca, Pascal Tanguy, coprésident du Digital club du Gepa et Yves Delafon, président du Gepa, lors du lancement qui s'est déroulé au Carré d'Aix. Photo M.D.

Le Groupement des entrepreneurs du pays d'Aix (Gepa) lance le Digital club. Une commission, coprésidée par Pascal Tanguy et Yves Curt, tous deux membres du Gepa, dont l'objectif est de sensibiliser les chefs d'entreprises à l'univers du numérique, dans une ambiance conviviale propice à des échanges entre les

acteurs du numérique pour qu'ils puissent, pourquoi pas, travailler ensemble. Chaque année, quatre soirées conférences seront proposées sur le thème du numérique.

La première conférence, animée par Ely de Travieso, président du Club de la sécurité des systèmes d'information régional (Clusir) Paca, a abordé *"la sécurité dans l'univers numérique"*. L'occasion de rappeler les obligations légales du chef d'entreprise qui, le plus souvent, ignore qu'il peut se retrouver en prison à cause d'un site internet, d'un réseau informatique ou encore d'un poste nomade.

Car la loi est claire : *"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."* La responsabilité du chef d'entreprise est donc bel et bien engagée et les menaces sont bien réelles.

De "belles" arnaques ont fait la une des journaux et les hackers ne manquent pas d'idées pour s'infiltrer dans les réseaux attirés par de l'usurpation d'identité, du vol de brevets, l'envoi de virus ou encore le cryptage des données de l'entreprise qui ne pourra les récupérer que moyennant une rançon... si elle n'a pas pris la précaution de les sauvegarder. Ce qui arrive encore ! Petites ou grosses entreprises, nulle n'est à l'abri et l'impact est loin d'être marginal aussi bien financièrement que commercialement ou encore au niveau de la réputation.

Se déresponsabiliser

Pour Ely de Travieso, il faut *"savoir accepter que le risque ne puisse être protégé à 100 % et se déresponsabiliser des risques légaux"*. Des solutions existent, même si elles ne sont pas toutes sûres à 100 % : politique de sécurité des services d'information (PSSI), audit, contrat garantissant un niveau de sécurité, authentification par un mot de passe difficile mélangeant chiffres, lettres et ponctuation, mais aussi les assurances, le cloud via des prestataires qui s'engagent à protéger les données, l'audit inversé en rémunérant des hackers rémunérés pour trouver les failles.

Il ne faut pas oublier de sécuriser son réseau Wi-Fi, verrouiller son smartphone ou sa tablette par un mot de passe, etc. Bref, tout faire pour décourager un hacker. Et surtout, séparer le professionnel du personnel.

Martine Debette