Chefs d’entreprise, particuliers, sécurisez vos données – L’écho du Mardi du 29 avril 2014

	**Chefs d’entreprise, particuliers, sécurisez vos données**Décryptage de l’Echo du Mardi du 29/04/2014. Propos recueillis par Mireille HURLIN.

Chefs d’entreprise, particuliers, sécurisez vos données – L’écho du Mardi du 29 avril 2014

Décryptage de l’Echo du Mardi du 29/04/2014. Propos recueillis par Mireille HURLIN.

DÉCRYPTAGE

Denis Jacopini est spécialiste de la cybercriminalité et en sécurité informatique. Il est, notamment, expert judiciaire en informatique près la Cour d'appel de Nîmes, consultant en sécurité informatique et en protection des données personnelles. Sa structure, Le Net expert Informatique de communication et conformité, se situe à Cavaillon.

« Chefs d'entreprise, particuliers, sécurisez vos données ! »

«Mon but est de sensibiliser les gens à l'existence, certes de risques mais surtout de protections qu'ils doivent respecter. Le but ? Que les usages de protection rentrent dans les mœurs sans se poser de question sur ce qu'il faut protéger. Que ca devienne une habitude d'utilisateur et que ca soit transparent. Internet est un monde, un outil propice aux pirates. Car ils ont tout le temps pour espionner un ordinateur, capter tout ce qu'il y a sur le disque dur, si les sécurités n'ont pas été mises en place. Lorsque l'on voit un intrus dans des locaux professionnels ou personnels, on intervient immédiatement. Or, on peut ne pas percevoir l'intrus dans l'ordinateur et du coup, le laisser agir sans le savoir. Ce que recherchent les pirates ? Les numéros de carte bancaire et les coordonnées personnelles que l'on peut avoir dans son ordinateur pour pouvoir aller pirater d'autres personnes. Posséder d'autres portes d'entrées vers d'autres utilisateurs. La plupart des attaques informatiques sont basées sur la confiance. On essaie d'utiliser la confiance de l'utilisateur, et au moment où il ne s'y attend pas, contaminer son ordinateur. Ça se passe aussi au niveau physique. Une personne arrive pour vendre quelque chose, elle va acquérir la confiance de son interlocuteur, boit un café avec la personne, puis se retrouve seule dans la pièce et dépose son petit appareil espion. Ça se passe aussi au niveau de l'ingénierie sociale. Les services de secrétariat ou administratifs sont contactés par des pirates qui se font passer pour des clients ou des fournisseurs pour acquérir des mots de passe, des numéros de compte. Ils peuvent ainsi, en trahissant la confiance que leur accordent les gens, obtenir des informations et des virements relativement importants. C'est ce qui s'est passé lorsque Bercy s'est fait pirater. Il s'agissait d'un mail qui provenait de quelqu'un de confiance qui a été reçu, ouvert, et qui a fait entrer un virus informatique dans le système. La voie était libre. Mon conseil pour les données qui sont stockées dans le Cloud ? Bien lire les conditions générales et vérifier ce qui est écrit sur les conditions de désengagement car elles sont rarement précisées. On devrait systématiquement prendre connaissance de ce qui se produit en cas de désengagement, au moment même de l'engagement pour être certain de conserver la main sur ses documents et sur les actions présentes et futures que l'on souhaite mener.»

Propos receuillis par Mireille Hurlin

Denis Jacopini nourrit son blog : www.lenetexpert.fr sur les sujets tels que les traitements de données personnelles, la sécurité informatique et la cybercriminalité et intervient aux côtés de Jean-Michel Abensour, avocat au Barreau d'Avignon sur de nombreux sujets du numérique sur la Web-radio intitulée Da vici code http://osmose-radio.e-monsite.com/pages/da-vici-code.html

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)