Les smartphones en questions

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 29 juin 2010

Iphone, Blackberry, Android.... Les téléphones intelligents ou « Smartphones » sont de plus en plus répandus et proposent des applications et des services variés.

Peut-on être pisté lorsqu'on utilise un Smartphone ou certaines applications ?

Les Smartphones récents sont pratiquement tous équipés d'une puce GPS. Il est ainsi techniquement possible de pister un téléphone. Il existe par exemple des applications permettant de localiser très précisément son téléphone en cas de perte, celui-ci transmettant des e-mails avec ses coordonnées GPS. La localisation permise est très précise. Néanmoins ces applications doivent être installées et activées par les utilisateurs, ce qui réduit le risque d'une utilisation malveillante.

Quels sont les autres risques encourus lors de l'utilisation d'applications ou de services sur un Smartphone ?

Il existe un risque de vol d'informations personnelles (localisation, mails, contacts, pièces jointes, ..) si l'utilisateur installe des applications malveillantes qui accèdent aux données du téléphone. Ainsi en 2009 une entreprise suisse a vu l'une de ses applications retirées de l'Appstore Iphone : celle-ci transmettait les coordonnées téléphoniques des acheteurs de l'application qui étaient ensuite démarchés par téléphone.

Que faire pour se prémunir de ces risques ?

Le premier réflexe à avoir est de faire attention aux applications que l'on installe sur son téléphone ; il faut aussi lire en détail les conditions d'utilisation des applications qui doivent préciser les données collectées et leur utilisation. En cas d'utilisation dans un contexte professionnel, les administrateurs ont la possibilité de limiter l'installation des applications à celles autorisées par l'entreprise. Et surtout, tous les utilisateurs doivent garder à l'esprit qu'un téléphone portable peut facilement se perdre, et qu'il doit donc impérativement être protégé par un code de verrouillage, après une courte période d'inactivité. Le code PIN de la carte SIM ne suffit pas.

Que font les fabricants pour protéger les utilisateurs ?

Les fabricants de Smartphones s'engagent vis-à-vis des applications disponibles sur leurs systèmes car bien évidemment les contrats qui lient les développeurs d'applications et les fabricants encadrent les collectes de données personnelles. Apple par exemple analyse les applications avant diffusion sur l'Appstore et a la possibilité d'effacer les applications à distance en cas de besoin.

Quelle est la spécificité des Blackberrys, téléphones les plus répandus dans le monde professionnel, par rapport aux autres Smartphones ?

Les Blackberry sont très appréciés dans le monde de l'entreprise pour leur capacité à recevoir des mails en mode 'push' : Ce mode de communication permet de recevoir des mails immédiatement après leur envoi, sans action manuelle. Ils permettent également la consultation de pièces jointes de façon efficace, car la plateforme Blackberry est capable de réduire la taille des documents afin de faciliter leur envoi sur le mobile. Pour cela, la plateforme Blackberry fait transiter les informations par le réseau de RIM [R i m], qui est le fabricant de ces téléphones. Cette

façon de faire est spécifique à RIM. En effet, les autres fabricants de smartphones ne font pas transiter les informations par leur réseau propre.

Cela peut-il poser des problèmes de sécurité des communications sur Blackberrys ?

Les Blackberrys souffrent en effet d'une mauvaise image en termes de sécurité. Les informations transmises depuis un BlackBerry transitent par les serveurs de RIM. Or, ces serveurs sont situés en Angleterre pour les utilisateurs européens, et au Canada pour les utilisateurs américains. Une polémique a éclaté en 2007 sur le fait que RIM pouvait potentiellement accéder aux informations et même les transmettre à la NSA, l'agence de renseignement américaine en charge des communications électroniques. RIM a mis fin à la polémique en fournissant des informations sur le fonctionnement de son système, et en apportant des garanties sur les mécanismes de chiffrement mis en place afin de garantir la confidentialité des informations.

A quel niveau intervient la CNIL sur cette problématique ?

Lorsqu'un service sur téléphone mobile est assuré par une entreprise située en France, celle-ci doit se conformer à la loi Informatique et Libertés et la CNIL peut notamment contrôler cette entreprise. Bien évidemment, cela ne dispense pas l'utilisateur d'être vigilant à l'égard des applications qu'il utilise.

Post-scriptum :

http://www.cnil.fr/la-cnil/actu-cni...