

RISK MANAGEMENT

L'I-PHONOPHOBIE DU RSSI...

Par Thierry Durand, Manager du pôle Audit et Conseil, NES

« Quand on eut bien considéré l'intérêt du public, celui de la partie, le résultat enfin de la suprême Cour fut de condamner la Folie à servir de guide à l'Amour », voilà près de 320 ans que Jean de La Fontaine donnait cette chute à sa fable « L'Amour et la Folie ». Gageons que, grand observateur de la vie de ses contemporains, il illustrerait aujourd'hui le même propos en publiant « L'iPhone et le RSSI », ou l'inverse, comme nous l'allons voir !



Thierry Durand, NES

L'iPhone est partout ! C'est un plébiscite ! Seuls quelques informaticiens ont encore des difficultés à le domestiquer. Il est apprivoisé par toutes les tranches d'âge, à la maison et dans l'entreprise, toutes cultures et toutes situations confondues ...

Mais la découverte quasi quotidienne des limites

que l'iPhone impose à la sécurité conduit le RSSI à rechercher des outils de protections complémentaires et le moyen de les mettre en œuvre.

Une liste de menaces qui ne cesse de s'allonger

Le RSSI a déjà identifié les menaces qui pèsent sur les PDA et les SMARTPHONES. La probabilité de les voir s'exercer sur l'iPhone est augmentée par le succès de l'appareil, mais aussi par sa connexion permanente à Internet, réseau dont la confiance n'est pas la première des qualités :

- Accès sans mot de passe, sauf choix à paramétrer,
- Solidité du mot de passe,
- Politique de gestion du mot de passe (renouvellement, etc.),
- Mot de passe administrateur 'standard' sauf remplacement volontaire,
- Protocole SSH accessible en WiFi sur appareils JailBreakés,
- Mot de passe messagerie mémorisé pour accès 'SSO',
- Robustesse du navigateur 'Safari',
- Filtrage des URLs,
- Virus et autres codes malveillants, en particulier sur

les i-Phone 'JailBreakés',

- Accès WiFi administrateur à toutes les données, sans traces exploitables,

• ...

L'iPhone fait peur au RSSI ! OUI, mais ... que peut-il faire ?

Peu de chance de voir des fonctionnalités de sécurité sur l'iPhone pour le moment...

Apple vise aussi le marché des Entreprises et ne manquera pas d'embarquer dans l'iPhone des solutions de durcissement et de protection efficaces... mais quand ? Et avec quelles limites ?

Il ne faut pas perdre de vue que l'iPhone fait l'unanimité parce qu'il est d'un usage simplissime et parfaitement intuitif. Toute évolution qui entacherait cette approche d'un quelconque relent d'informatique « traditionnelle » le ramènerait immédiatement au rang des Smartphones sous Windows 6 ou des BlackBerry. L'avantage étant alors perdu, l'ambition de pénétrer l'entreprise ne serait plus de mise !

Alors peut-on raisonnablement attendre d'Apple des réponses complètes aux frayeurs du RSSI qui voit déjà fuir les données de l'entreprise ? Probablement pas ! En tout cas, pas tant qu'un concurrent aussi habile en présentation ne proposera pas un niveau de sécurité très supérieur !

...Et la marge de manœuvre du RSSI est étroite

Comme il le fait dans l'Entreprise, le RSSI voudrait imposer une politique de mot de passe, se réserver l'autorité d'administrateur, organiser les contrôles d'accès,

RISK MANAGEMENT



garantir l'intégrité et la confidentialité, ..., en un mot, appliquer la Politique de Sécurité du Système d'Information de l'entreprise aux données qui transitent sur les iPhone de son personnel.

En a-t-il les moyens ?

Il est probable que des solutions verront progressivement le jour pour répondre aux préoccupations du RSSI, mais alors restera-t-il un réel intérêt pour l'employé-usager à disposer d'un iPhone plutôt que d'un Smartphone ou d'un BlackBerry ? Et pour l'entreprise, pourquoi s'engager dans cette voie mal balisée alors que les mêmes fonctions résultantes sont déjà servies par d'autres équipements maîtrisés et performants ?

Aujourd'hui, il semble bien que la demande vienne de l'utilisateur plutôt que de l'employeur !

Et si, malgré l'équipement professionnel qui lui a été remis, l'employé-usager choisit à titre privé d'utiliser un iPhone ? Qui saura lui imposer des solutions de protection ? Qui saura l'empêcher d'y faire transiter des données de l'Entreprise ?

Toutes les entreprises qui ont ouvert des accès 'web' à leur messagerie vont voir leurs iPhoneistes diriger leur courrier vers leur iPhone (en mémorisant au passage leurs identifiants d'accès professionnel) !

NON, décidément, le RSSI ne peut pas imposer les solutions qu'il juge nécessaires, d'autant que les risques viennent tout autant des iPhone privés sur lesquels l'Entreprise n'a pas de prise.

Où est la faille ?

Voilà des années que l'Entreprise laisse ses employé(e)s (cadres notamment) transporter des documents professionnels dans leur sac à main ou dans leur attaché-case. Ces objets de maroquinerie, privés et parfois luxueux, n'ont jamais été interdits dans l'Entreprise et leur robustesse n'y a jamais été contrôlée avant d'y autoriser le transport de documents.

L'iPhone ne serait-il pas le premier né d'une génération de sacs à main numériques ou d'attachés-cases électroniques ?

La question est pertinente si l'on songe à ce qu'il permet de ranger : photos, vidéos, musiques, documents, courriers, agenda, bloc-notes, répertoire, boussole, plans et cartes, journaux, magazines et presse, calculatrice, et tellement d'autres choses... et même un téléphone !

Sans compter que d'innombrables 'applications' viennent chaque jour enrichir cet inventaire à la Prévert ! Regardez les possesseurs d'iPhone, dans la rue, dans le train ou le métro, dans le bus, au bureau, à la maison ... ils l'ont 'en main', ce n'est ni un 'jouet' ni un 'outil', c'est juste une sorte de 'prolongement d'eux-mêmes' !

Laisser l'entreprise installer des protections sur son iPhone serait vécu par son 'maître' comme lui imposer une carapace ou, pire encore, lui greffer des organes !

Et la sécurité dans tout ça !

Nous étions nombreux à répéter depuis des années que le « risque majeur » était installé entre la chaise et le clavier. Le clavier était alors le 'point d'entrée' du SI de l'Entreprise, le premier maillon 'non humain' de la chaîne d'accès au SI.

Avec l'arrivée de l'iPhone, c'est ce maillon qui est remis en cause. L'utilisateur et l'iPhone tentent, ensemble, de ne faire qu'un ... mais l'iPhone accède directement au SI ! Le « risque majeur » n'est plus installé entre la chaise et le clavier, il est installé entre la chaise et ... le SI lui-même ! Avec tout ce qui a été dit sur l'iPhone et son usage en toute liberté, n'est-ce pas « folie » que de le laisser accéder au SI ?

Bien sûr, le SI est protégé et va étendre sa protection à ce nouveau mode d'accès, mais on voit bien que c'est très insuffisant.

Jean de la Fontaine suggérait que la Folie soit un guide pour l'Amour ; ne devrait-on pas espérer que l'iPhone et son maître devienne(nt) lui(eux)-même(s) un guide pour le RSSI ?

Quand le comportement de l'homme (et de son iPhone) est un risque sans parade ou protection possible, c'est la sensibilisation de l'utilisateur qui doit réduire le risque.

Le RSSI doit se laisser guider par l'iPhone pour apprendre à chaque utilisateur à se protéger lui-même des dangers qui le guettent, à devenir 'prudent'.

« Prudence est mère de Sûreté » ... qui aurait bien pu dire cela ?



THE ISSM AND IPHONE PHOBIA

By THIERRY DURAND, MANAGER OF THE AUDIT AND CONSULTING DIVISION, NES



Jean de La Fontaine's fable 'Love & Folly', written 320 years ago, ends with the lines 'When the gods had each well considered the public interest on the one hand and the complainant's demands upon the other, the supreme court gave as its verdict that Folly was condemned for ever more to serve as a guide for the footsteps of Love'. The behaviour of La Fontaine's contemporaries that inspired this fable could well be illustrated today with a fable entitled 'The iPhone and the ISSM' -- or maybe the reverse, as we shall see below!