Reportage: comment Microsoft sécurise – où l'histoire du « Wild Wild Web »

Redmond.– La presse européenne est conviée ici durant deux jours pour mieux connaître la **stratégie sécurité de Microsoft.** Une plongée dans le sanctuaire de l'éditeur de Windows, au bord du Pacifique sur les côtes de Seattle.

Où l'internaute met-il les pieds ? Voilà le *leitmotiv*auquel Microsoft se raccroche – à en croire ses représentants. Les spécialistes se succèdent au pupitre pour exposer la position de l'éditeur et donner une vision prospective de ce que sera demain la sécurité d'Internet.

George Stathakopoulos, responsable de la division des produits Sécurité évoque ainsi l'évolution des menaces Web et leur impact sur les infrastructures:

« *Si protéger le consommateur a toujours été notre simple objectif, force est de constater que* ***l'explosion d'Internet a considérablement changé la donne****. Le village global a changé la donne*« .

On s'aperçoit alors que l'histoire des « bons » et des « méchants » digne du Far-West a toujours été d'actualité sur le Net.

Le haut responsable Sécurité, à Redmond depuis 1991, en relate la typologie: « *Dès 1998, on a pu voir nombre d'attaques de type*« défacements *» qui ont contribué à la création de véritables groupes de hackers à travers le monde*« . Il faut dire que la **vulnérabilité des OS, Windows en premier lieu, permettait facilement aux intrus de faire leur marché**. Le désir de certains hackers de passer à la postérité va alors contribuer à faire entrer le piratage dans l'ère des vers.

« *Les vers [worms] et leur utilisation ont contribué a créer une spécialisation des compétences. Des capacités différentes sont utilisées entre celui qui crée le ver et celui qui le diffuse.****Il est alors d'autant plus difficile d'établir des contre-mesures efficaces*****«** .

George Stathakopoulos poursuit:

« *La dernière phase est celle des*botnets*. L'avènement des sites de vente en ligne depuis 2004 a engendré un attrait vers les gains financiers possibles du piratage. Une orientation qui se propage aux réseaux sociaux* « .

Des attaques ciblées grâce aux informations collectées semblent être le credo des « *bad guys »* (« les méchants »). La dissémination des informations contribue donc à rendre l'espionnage informatique rentable pour les pirates.

De même, la multiplication des faux logiciels de sécurité par exemple pose la question de la confiance qu'ont les utilisateurs envers leurs outils. Brendon Lynch, directeur de la stratégie vie privée de Microsoft pose le problème : « *Si* ***Internet a modifié notre manière de communiquer*** *reste que le*privacy *est devenu un impératif économique mais aussi social. Il y a donc un réel besoin de modifier la politique qu'ont les professionnels sur l'échange d'informations. On pourrait imaginer de tenter de 'dévaluer' les informations aux yeux des hackers*« .

Une question déjà évoquée par les experts français en sécurité. Déjà en 2000, Microsoft avait eu l'idée de créer le Passport.net afin d'établir une identité complète d'un utilisateur connecté sur la toile. Plus près de nous, Microsoft toujours a mis en place dans Vista le **Windows Card Space.** Cet outil fournit alors une véritable carte d'identité virtuelle. Citons **également OpenID de Yahoo.**

Depuis lors, l **'essor des réseaux sociaux a amplifié le phénomène** avec une accumulation de formulaires d'inscription et donc d'enregistrement des données éparpillées sur plusieurs domaines…

Un contexte que commente Brendon Lynch:

« *Avoir une* ***gouvernance globale coûte de l'argent*** *mais il est évident qu'il faudra une conciliation* ». Demeure la question de la préservation de ces données et de leur destruction. Un enjeu pour lequel chacun des géants semble tirer la couverture ou plutôt le parapluie à soi… chacun de son côté.