Quelle entreprise peut encore faire confiance à Microsoft ? par Glyn Moody

Le titre se suffit à lui-même ici. On pourrait ajouter aux entreprises, les institutions et les particuliers, bref tout le monde.

Non content d'avoir été accusé par le passé de réserver dans Windows des portes dérobées à la NSA, non content d'être fortement suspecté de laisser les autorités américaines collecter nos données dans Skype, Microsft est maintenant soupçonné de différer la publication de ses patchs de sécurité pour en informer d'abord les mêmes autorités américaines !

Tout DSI normalement constiué(e) devrait lire cet article et en tirer avec sa direction ses propres conclusions.

Quelle entreprise peut encore faire confiance à Microsoft ?

How Can Any Company Ever Trust Microsoft Again?

Glyn Moddy – juin 2013 – Open Enterprise (Computer World)
(Traduction : Slystone, Luo, lamessen, Antoine, sinma, Pouhiou, Sky, Fe-lor, aKa, Asta, audionuma + anonymes)

Quels que soient les détails des récentes révélations sur l'espionnage de masse de la part des États-Unis fournis par Edward Snowden dans le Guardian, il y a déjà un énorme bénéfice collatéral. D'un côté, le gouvernement des États-Unis se replie sur lui-même, niant certaines allégations en offrant sa propre version de l'histoire. Cela, et pour la première fois, nous donne des détails officiels sur des programmes dont nous n'étions (au mieux) informés que par fuites et rumeurs, voire pas du tout. De plus, la précipitation indécente et l'histoire sans cesse changeante des autorités américaines est une confirmation, si elle était encore nécessaire, que ce que Snowden a révélé est important – vous ne provoquez pas un tel tapage pour rien.

Mais peut-être encore plus crucial, d'autres journalistes, poussés par la honte et leur culpabilisation, ont finalement posé des questions qu'ils auraient dû poser des années voire des décennies plus tôt. Cela a abouti à une série d'articles extrêmement intéressants à propos de l'espionnage de la NSA, dont beaucoup contiennent des informations auxiliaires qui sont aussi intéressantes que l'histoire principale. Voici un bel exemple de ce qui est apparu durant le week-end sur le site de Bloomberg.

Entre autres choses, il s'agit de Microsoft, et d'évaluer dans quelle mesure ils ont aidé la NSA à espionner le monde. Bien sûr, cette crainte n'est pas nouvelle. Dès 1999, il était déjà dit que des portes dérobées avaient été codées dans Windows :

> *Une erreur d'inattention de programmeurs Microsoft a révélé qu'un code d'accès spécial préparé par l'agence nationale de sécurité étasunienne (NSA) avait été secrètement implémenté dans Windows. Le système d'accès de la NSA est implémenté sous toutes les versions de Windows actuellement utilisées, à l'exception des premières versions de Windows 95 (et ses prédécesseurs). La découverte suivait de près les révélations survenues un peu plus tôt cette année concernant un autre géant du logiciel étasunien, Lotus, qui avait implémenté une trappe « d'aide à l'information » pour la NSA dans son système Notes. Des fonctions de sécurité dans d'autres logiciels systèmes avaient été délibérément paralysées.*

Plus récemment, il y eut des craintes au sujet de Skype, racheté par Microsoft en mai 2011. En 2012, il y a eu des discussions pendant lesquelles on s'est demandé si Microsoft avait changé l'architecture de Skype pour rendre l'espionnage plus facile (l'entreprise a même un brevet sur l'idée). Les récentes fuites semblent confirmer que ces craintes étaient bien fondées, comme le signale Slate :

> *Le scoop du Washington Post sur PRISM et ses possibilités présente plusieurs points frappants, mais pour moi un en particulier s'est démarqué du reste. The Post, citant une diapositive Powerpoint confidentielle de la NSA, a écrit que l'agence avait un guide d'utilisation spécifique « pour la collecte de données Skype dans le cadre du programme PRISM » qui met en évidence les possibilités d'écoutes sur Skype « lorsque l'un des correspondants utilise un banal téléphone et lorsque deux utilisateurs du service réalisent un appel audio, vidéo, font du chat ou échangent des fichiers. »*

Mais même cela devient dérisoire comparé aux dernières informations obtenues par Bloomberg :

> *D'après deux personnes qui connaissent bien le processus, Microsoft, la plus grande compagnie de logiciels au monde,*

> *fournit aux services de renseignement des informations sur les bogues dans ses logiciels populaires avant la publication d'un correctif. Ces informations peuvent servir à protéger les ordinateurs du gouvernement ainsi qu'à accéder à ceux de terroristes ou d'armées ennemies.*
>
> *La firme de Redmond basée à Washington, Microsoft, ainsi que d'autres firmes œuvrant dans le logiciel ou la sécurité, était au courant que ce genre d'alertes précoces permettaient aux États-Unis d'exploiter des failles dans les logiciels vendus aux gouvernements étrangers, selon deux fonctionnaires d'État. Microsoft ne demande pas et ne peut pas savoir comment le gouvernement utilise de tels tuyaux, ont dit les fonctionnaires, qui ne souhaitent pas que leur identité soit révélée au vu de la confidentialité du sujet.*
>
> *Frank Shaw, un porte-parole de Microsoft, a fait savoir que ces divulgations se font en coopération avec d'autres agences, et sont conçues pour donner aux gouvernements « une longueur d'avance » sur l'évaluation des risques et des mitigations.*

Réfléchissons-y donc un moment.

Des entreprises et des gouvernements achètent des logiciels à Microsoft, se reposant sur la compagnie pour créer des programmes qui sont sûrs et sans risque. Aucun logiciel n'est complètement exempt de bogues, et des failles sérieuses sont trouvées régulièrement dans le code de Microsoft (et dans l'open source, aussi, bien sûr). Donc le problème n'est pas de savoir si les logiciels ont des failles, tout bout de code non-trivial en a, mais de savoir comment les auteurs du code réagissent.

Ce que veulent les gouvernements et les compagnies, c'est que ces failles soient corrigées le plus vite possible, de manière à ce qu'elles ne puissent pas être exploitées par des criminels pour causer des dégâts sur leurs systèmes. Et

pourtant, nous apprenons maintenant que l'une des premières choses que fait Microsoft, c'est d'envoyer des informations au sujet de ces failles à de multiples agences, en incluant sans doute la NSA et la CIA. En outre, nous savons aussi que « ce type d'alerte précoce a permis aux U.S.A. d'exploiter des failles dans les logiciels vendus aux gouvernements étrangers »

Et rappelez-vous que « gouvernements étrangers » signifie ceux des pays européens aussi bien que les autres (le fait que le gouvernement du Royaume-Uni ait espionné des pays « alliés » souligne que tout le monde le fait). Il serait également naïf de penser que les agences de renseignement américaines exploitent ces failles « jour 0 » seulement pour pénétrer dans les systèmes des gouvernements ; l'espionnage industriel représentait une partie de l'ancien programme de surveillance Echelon, et il n'y a aucune raison de penser que les U.S.A. vont se limiter aujourd'hui (s'il y a eu un changement, les choses ont empiré).

Il est donc fortement probable que les faiblesses des produits Microsoft soient régulièrement utilisées pour s'infiltrer et pratiquer toutes sortes d'espionnage dans les gouvernements et sociétés étrangères. Ainsi, chaque fois qu'une entreprise installe un nouveau correctif d'une faille majeure provenant de Microsoft, il faut garder à l'esprit que quelqu'un a pu avoir utilisé cette faiblesse à des fins malveillantes.

Les conséquences de cette situation sont très profondes. Les entreprises achètent des produits Microsoft pour plusieurs raisons, mais toutes supposent que la compagnie fait de son mieux pour les protéger. Les dernières révélations montrent que c'est une hypothèse fausse : Microsoft transmet consciencieusement et régulièrement des informations sur la manière de percer les sécurités de ses produits aux agences américaines. Ce qui arrive à ces informations plus tard est, évidemment, un secret. Pas à cause du « terrorisme », mais parce qu'il est presque certain que des attaques illégales

sont menées contre d'autres pays (et leurs entreprises) en dehors des États-Unis.

Ce n'est rien d'autre qu'une trahison de la confiance que les utilisateurs placent en Microsoft, et je me demande comment un responsable informatique peut encore sérieusement recommander l'utilisation de produits Microsoft maintenant que nous sommes presque sûrs qu'ils sont un vecteur d'attaques par les agences d'espionnage américaines qui peuvent potentiellement causer d'énormes pertes aux entreprises concernées (comme ce qui est arrivé avec Echelon).

Mais il y a un autre angle intéressant. Même si peu de choses ont été écrites à ce sujet – même par moi, à ma grande honte – un nouvel accord législatif portant sur les attaques en ligne est en cours d'élaboration par l'Union Européenne. Voici un aspect de cet accord :

> *Ce texte demandera aux États membres de fixer leur peine maximale d'emprisonnement à au moins deux ans pour les crimes suivants : accéder à ou interférer illégalement avec des systèmes d'informations, interférer illégalement avec les données, intercepter illégalement des communications ou produire et vendre intentionnellement des outils utilisés pour commettre ces infractions.*

« Accéder ou interférer illégalement avec des systèmes d'informations » semble être précisément ce que le gouvernement des États-Unis fait aux systèmes étrangers, dont probablement ceux de l'Union Européenne. Donc, cela indiquerait que le gouvernement américain va tomber sous le coup de ces nouvelles réglementations. Mais peut-être que Microsoft aussi, car c'est lui qui en premier lieu a rendu possible l'« accès illégal ».

Et il y a un autre aspect. Supposons que les espions américains utilisent des failles dans les logiciels de Microsoft pour entrer dans un réseau d'entreprise et y

espionner des tiers. Je me demande si ces entreprises peuvent elles-mêmes se trouver accusées de toute sorte d'infractions dont elles ne savaient rien ; et finir au tribunal. Prouver son innocence ici risque d'être difficile, car en ce cas les réseaux d'entreprise seraient effectivement utilisés pour espionner.

Au final, ce risque est encore une autre bonne raison de ne jamais utiliser des logiciels de Microsoft, avec toutes les autres qui ont été écrites ici ces dernières années. Ce n'est pas uniquement que l'open source est généralement moins cher (particulièrement si vous prenez en considération le prix de l'enfermement livré avec les logiciels Microsoft), mieux écrit, plus rapide, plus sûr et plus sécurisé. Mais par-dessus tout, le logiciel libre respecte ses utilisateurs, les plaçant solidement aux commandes.

Cela vous ôte toute crainte que l'entreprise vous ayant fourni un programme donne en secret à des tiers la possibilité de retourner contre vous ce logiciel que vous avez payé assez cher. Après tout, la plupart des résolutions des bogues dans l'open source est effectuée par des codeurs qui ont un peu d'amour pour l'autorité verticale, de sorte que la probabilité qu'ils donnent régulièrement les failles à la NSA, comme le fait Microsoft, doit être extrêmement faible.

Crédit photo : Cambodia4kidsorg (Creative Commons By)