Edward Snowden et les portes dérobées

Grâce aux révélations d'Edward Snowden, on a su que la NSA tentait et réussissait parfois à introduire des portes dérobées dans certains programmes de cryptographie (comme celui d'un générateur pseudoaléatoire du NIST), se donnant ainsi la possibilité de déchiffrer facilement les communications de ceux qui les utilisaient : la NSA espionnait ainsi des citoyens américains, ce que les lois des États-Unis interdisent pourtant.

Le film *Snowden* du réalisateur Oliver Stone est sorti en 2016. Il retrace les péripéties de ce lanceur d'alerte toujours recherché par la police des États-Unis et aujourd'hui réfugié en Russie.

Récemment encore, une vieille idée pourtant combattue par tous les spécialistes de sécurité informatique a resurgi. Deux sénateurs américains, Richard Burr et Dianne Feinstein, ont déposé un projet de loi qui forcerait tous les acteurs des technologies de l'information à truffer de portes dérobées leurs matériels et logiciels. Le projet voulait accorder aux tribunaux américains le pouvoir d'exiger des entreprises telles que Microsoft, Apple, Google, Facebook, etc. qu'elles donnent accès à toutes les données des appareils qu'elles vendent et des services qu'elles offrent.

Comme c'est le cas depuis longtemps maintenant, un grand nombre d'experts se sont élevés contre cette idée qui, si elle était adoptée, reviendrait à affaiblir gravement tous les systèmes de sécurité pourtant de plus en plus nécessaires qui protègent les informations des particuliers et des entreprises. Comme l'écrivaient Pauline Glikman et Nicolas Glady de l'Essec (École supérieure des sciences économiques et commerciales) le 27 mai 2016 dans une tribune sur www.silicon.fr : « Si ce projet de loi américain était voté, les entreprises européennes se verraient donc dans l'obligation d'abandonner l'usage des appareils et services informatiques des fournisseurs américains. Ce serait un coup majeur porté à la compétitivité des États-Unis, qui verraient leurs clients se tourner vers les services chiffrés offerts par des entreprises non soumises à ces contraintes... »

Même aux États-Unis, où l'on sait que les révélations d'Edward Snowden ont déjà affaibli la confiance dans les entreprises et produits nationaux, le projet de loi fait l'objet de très vives critiques. Reste qu'il n'y a aujourd'hui aucun doute que les systèmes d'écoute et d'espionnage massifs mis en place par la NSA au niveau mondial sont un problème pour la souveraineté de tous les États, en même temps qu'un danger économique majeur... et que ces systèmes n'ont pas été désactivés.

la destruction simultanée de tous les gants. Certes, les autorités ne devraient utiliser ce message radio secret que dans des enceintes fermées ne laissant pas échapper le signal destructeur, et uniquement dans le but de s'attaquer à des gants mêlés à des affaires de banditisme ou de terrorisme, mais comment ne pas craindre un accident ou un détournement ?

Le FBI contre Apple

Ces questions ont récemment défrayé la chronique à propos des téléphones d'Apple. En février 2016, le FBI (*Federal Bureau of Investigation*, la police judiciaire américaine) demanda à Apple de l'aider à rendre accessibles les données du téléphone d'un des auteurs de la tuerie de décembre 2015 à San Bernardino, où 14 personnes périrent. Le problème n'était pas directement celui d'une porte dérobée, mais il se fondait sur l'idée très proche que le système de protection des téléphones d'Apple pouvait être contourné avec l'aide des ingénieurs d'Apple. En clair, le FBI ne doutait pas qu'une sorte de porte dérobée existait et demandait à Apple de la faire fonctionner pour lui livrer le contenu du téléphone.

Apple répondit qu'il ne voulait pas collaborer, non pas que cela fût pour lui impossible, mais parce que cela aurait été contraire à l'intérêt de ses clients. Plus précisément, le FBI demandait à Apple de lui donner un moyen d'éviter que ne fonctionne le système d'effacement automatique qui s'enclenche en cas de tentatives répétées d'accès aux données de l'appareil.

Tim Cook, le président d'Apple, a expliqué : « Le gouvernement des États-Unis a exigé qu'Apple prenne une mesure sans précédent qui menace la sécurité de nos clients. Nous ne voulons pas nous soumettre à sa demande, car cela aurait des conséquences bien au-delà du cas particulier concerné. La situation exige un débat public ; nous voulons que nos clients et tous les gens à travers le pays comprennent ce qui est en jeu. »

Quelques jours plus tard, l'affaire trouva un épilogue décevant et inquiétant pour les clients d'Apple : le FBI, avec une aide dont l'identité est restée cachée, réussit à accéder aux données du téléphone. Ce dénouement signifie tout simplement que les protections prétendues inviolables des téléphones d'Apple ne le sont pas, soit parce qu'un tiers sait les contourner, soit parce