‘Patchs’: quelle politique raisonnable d’information et de diffusion ?

Ces dernières années, la question de la politique de diffusion d’information concernant une vulnérabilité a souvent été posée. De nombreuses approches existent, intéressantes pour certaines, clairement corporatistes pour d’autres. Les mots à la mode sont le ‘Full Disclosure’ ou le ‘Responsible Disclosure’. La bataille se porte sur le contrôle d’une information sensible, permettant de potentiellement compromettre des ordinateurs qui ne sont pas encore protégés.

Un exemple. Le correctif Microsoft MS05-019 (KB893066), qui fixe plusieurs problèmes de sécurité, désactive silencieusement une fonction importante de la pile TCP/IP. La question de l’information en matière de sécurité touche donc également les correctifs distribués par les éditeurs. Si des politiques de diffusion d’informations sensibles sur les vulnérabilités existent, une politique raisonnable d’information et de diffusion de correctifs serait un quasi-devoir pour les éditeurs de logiciels. Suite à ce patch de Microsoft, le comportement de la pile IP a subi une lourde modification. L’accès brut aux données réseaux de bas niveau (Raw Sockets) a tout simplement été supprimé et certaines applications, notamment des logiciels de sécurité, ne fonctionnent plus sur les machines « patchées ». Le problème ici n’est pas tant le changement de fonctionnalité, ni son installation silencieuse par Windows Update, ou encore le manque de communication de l’éditeur de Redmond sur ce ‘bundle’, mais bel et bien l’association d’une « désactivation de fonctionnalité » avec la « correction de vulnérabilités » en un seul et unique patch. **Confiance et alternatives ?** Ce genre d’incident, vivement décrié par la communauté, ne fait que diminuer la confiance des utilisateurs vis a vis des correctifs et autres services packs qui sont mis à disposition du public et des entreprises. Le problème de changement de fonctionnalité avait donné assez mauvaise presse au Service Pack 2 de Windows XP, au point que de nombreuses sociétés ne l’ont pas déployé. Une des préoccupations principales des responsables de systèmes d’information est la sécurité mais également, et surtout, la faculté de l’utilisateur à être productif avec son principal outil de travail, son ordinateur. Les services informatiques essaient au maximum de réduire les sources de problèmes pour les postes de travail. L’objectif étant de diminuer le temps passé en assistance utilisateur et en dépannages, si une nouvelle source de chaos telle que ce type de problématique se renouvelle, les administrateurs vont finir par s’arracher les cheveux. **En prenant soin de sélectionner** Cette méfiance apporte de l’eau au moulin des responsables informatiques qui délaissent le ‘patching’ coûteux et dangereux, même s’il est assisté par une solution de ‘Patch Management’. Certains choisissent de n’appliquer que quelques correctifs soigneusement sélectionnés et équipent leurs systèmes avec des produits dits de ‘Desktop Security’ tels que des ‘Personal Firewalls’ ou ‘Host Intrusion Prevention’. Cette démarche semble assez efficace car elle combine les correctifs vitaux avec une protection générique contre les nouvelles formes d’attaques utilises par les crackers, les spywares et les backdoors. La situation actuelle a été assez bien résumée par l’auteur de Nmap, un des outils favori de la communauté et affecté par ce patch : *« Voici le dilemme, choisissez votre poison: installez le dernier hotfix de Microsoft et dégradez votre système ou ignorez le patch et soyez vulnérable à du déni de service et des intrusions par le réseau »*. Plus d’infos: http://seclists.org/lists/nmap-hackers/2005/Apr-Jun/0000.html (*) **pour Vulnerabilite.com**