Microsoft veut renouer avec ‘l’informatique de confiance’

2001, catastrophe planétaire pour Microsoft, qui doit affronter une vague d’attaques virales. Le socle de confiance dont bénéficiait l’éditeur s’effrite. Pour regagner l’attention de ses clients, Microsoft doit réagir très vite. Ce fut le projet de l’informatique de confiance. Lancé en janvier 2002, sa mission est d’envergure, car elle doit engendrer chez l’éditeur un changement culturel en profondeur, en faisant de la sécurité la priorité stratégique du groupe. Un changement des mentalités qui s’inscrit dans la durée. La nouvelle stratégie de Microsoft se résume en une formule : SD3+C. « Secure by Design x Secure by Default x Secure in Deployment + Communications ». – Réduire les vulnérabilités dans le code avec SDL (Security Development Lifecycle) ; – Réduire la surface d’attaque avec les paramétrages par défaut ; – Former les individus et déployer les correctifs ; – Communiquer. Et trois ans après ? Quel sont les effets de ce changement culturel? Deux tendances tendent à démonter que Microsoft est sur la bonne voie : le nombre des bulletins de sécurité se réduit, ainsi que les temps de réactivité face aux attaques et aux failles. Certes, l’éditeur reste la cible à la fois des hackers et des médias. Difficile dans ces conditions d’échapper aux menaces ! Les retours d’expérience de ses clients permettent à Microsoft d’évaluer à 1,5 milliard le nombre de ‘crashes’ de PC sous Windows par an. Un chiffre qui reste élevé, mais pas tant que cela si on le rapporte à la base installée. Mais, c’est toujours trop ! Si le travail effectué est gigantesque, il n’est pas non plus dépourvu de limites. En particulier, nombre de vulnérabilités n’ont pas été corrigées, et ne le seront pas ! Il est souvent préférable de faire le choix d’avancer, plutôt que de revenir en arrière ! Mais c’est aussi certainement du côté des utilisateurs qu’il faut rechercher des causes profondes aux défauts de fiabilité des systèmes. Ils multiplient en effet les fonctionnalités associées aux services, ce qui multiplie de fait leur fragilité ! Et la gestion du système d’information se révèle aussi complexe, fruit de l’hétérogénéité. Encore bien du chemin à parcourir Il reste donc de nombreuses missions à accomplir : – mettre en ?uvre des mesures de défense en profondeur ; – déployer les mesures de sécurité de manière plus efficace ; – étendre la gestion des accès à l’entreprise étendue afin d’élargir son paramètre de sécurité ; – réduire la fréquence des mises à jour de sécurité ; – et conseiller sur la sécurisation des systèmes. Dans ce plan stratégique, en dehors des technologies toujours perfectibles, on constate la présence du maillon faible de la chaîne de sécurité, l’utilisateur. Celui-là même qu’il est le plus difficile d’accompagner ! La mise en place par défaut des mesures et outils de sécurité s’adresse directement à eux. L’annonce d’ISA Server 2005 Enterprise (lire notre article) entre d’ailleurs dans cette stratégie. Il s’agit ici de travailler sur l’isolation et la résilience. L’isolation, c’est la réduction du risque lié à la surface et aux vecteurs d’attaques. La résilience, c’est l’intégration des technologies de protection dans le périmètre des sécurités applicatives. Deux développements marquent cette évolution chez Microsoft, le SP2 de Windows XP, avec ses 130 millions de déploiements, et Windows AntiSpyware, qui devrait rester gratuit en utilisation personnelle, mais passer sur un modèle payant pour les entreprises. Un pas important a été franchi par Microsoft, mais la dimension de celui qui reste à franchir est loin d’être défini !