Reportage : génèse d'un 'patch' chez Microsoft

Redmond. – Lors d'une rencontre avec la presse européenne, ici au siège de Microsoft, des ingénieurs R&D ont évoqué le processus d **'élaboration du système de sécurité « maison ».** Plusieurs étapes sont nécessaires afin d'organiser la parade à une vulnérabilité.

Si la partie visible de l'iceberg reste les ***'patch Tuesdays'***, force est de reconnaître que les équipes du MSRC (Microsoft Security Response Center) ont mis en place un système de réponse aux failles qui leur permet de **répondre en 24 heures à une demande d'un particulier ou d'un professionnel.**

Concernant les fameux '*patchs*', Mike Reavey, directeur de ce labo MSRC décrit ainsi les premières étapes du processus:

« *Tout commence par le rapport de vulnérabilité. Lorsqu'une faille nous parvient, la phase qui va mener à une solution peut alors commencer. Chacun peut envoyer et expliquer son problème à l'adresse* ***secure@microsoft.com****. L'e-mail peut être anonyme dans le sens où nous ne recherchons pas à connaître l'identité de l'expéditeu*r ».

Commence alors la phase de **triage**. Ici aussi, le responsable en explique les détails : *« Faire le tri nous permet d'y voir plus clair dans la forêt de messages que nous recevons. Il est alors crucial de* ***comprendre l'importance de la vulnérabilité ciblée afin de mieux la calibrer*****« .**

Sa collègue, la sémillante Sarah Blankinship acquiesce. Elle continue la démonstration, en relatant les détails du processus :

« *La suite du process concerne la nécessité de* ***trouver une réponse aux questions posées.*** *En ce sens, nous travaillons en équipe afin d'établir la meilleure solution possible. On fait d'abord* ***un test en interne pour savoir si les solutions fonctionnent****. Ensuite on les applique et les envoie*« . Il reste alors aux professionnels de Redmond à réaliser le contenu de sécurité – l'écriture de la solution.

Afin de mutualiser les efforts, les équipes ont mis en place le **MAPP** (Microsoft Active Protection Program). Un réseau de partenaires-membres avec lesquels les responsables de Redmond vont **communiquer plus facilement** afin d'établir un échange d'informations plus rapide.

Mike Reavey témoigne : « *Les membres reçoivent nos* ***informations un mois à l'avance****. Cela leur permet de nous communiquer des informations, voire des parades bien utiles…* »

Même constat de Damian Hasse, responsable principal de la sécurité, à propos du cycle de *patchs* : « S*'il n'y a* ***pas de temps moyen pour évaluer et éditer une solution qui aboutira à un patch,*** *concernant le MS08-025* [vulnérabilité signalée confidentiellement dans le noyau Windows], *le temps a été plutôt long. On a eu le 'drapeau rouge' le 26 octobre et le patch a été diffusé le 11 avril*« .

Il conclut, « *le délai peut être réduit selon si on a identifié correctement les risques*« .

Un tel cycle promet de se perpétuer à l'avenir. Dan Kaminsky, l'expert au centre de la **faille DNS** a

estimé que si le système n’était pas le meilleur, il restait, à l’heure actuelle le lus rapide…