Windows 7 et sécurité: D. Leland, Microsoft explique la « dépérimètrisation »

« *Avec la sortie de Windows 7, la sécurité est évidemment un domaine important, qui couvre un large spectre sur toute notre offre, et pas seulement Windows 7*« , insiste d'entrée de jeu, Douglas Leland.

Pour résumer, rappelons q'une nouvelle méthodologie « sécurité » a été introduite il y a 3 ou 4 ans, lorsque Bill Gates a tapé du poing sur la table et demandé explicitement que tous les développements soient repensés selon un cycle de vie spécifique : '***security design lifecycle***'.

Et Douglas Leland d'expliquer:

« *Ces derniers mois, le groupe que je dirige, « Security solutions », s'est concentré sur toutes les menaces particulières ('*special threats*') que nous avons pu identifier. Nous avons également beaucoup travaillé sur l'authentification des utilisateurs et sur les technologies de contrôle d'accès au Web*. » (cf. article Security Essentials)

La nouvelle tendance? C'est ce qu »on appelle la '**dépérimètrisation**« : « *Cela consiste à gérer plus facilement et de façon plus souple toute extension de connexion de PC ou postes téléphoniques. Dans le précédent modèle, on était obligé de définir des zones protégées par des 'firewalls' (pare-feux), des systèmes d'authentification placés à chaque passerelles d'accès, des VPN (réseaux privés virtuels), etc. Donc toute nouvelle connexion, y compris en mobilité extérieure nécessitait de reconstruire, au moins en partie, le dispositif de sécurité en place.* »

A l'inverse, une stratégie de périmètre élargi permet d'ouvrir le réseau quasi instantanément. L'administrateur a seulement besoin de connecter les équipements à distance, car tous les points de connectivité réseau et toutes les données seraient a priori sécurisés de façon intrinsèque par des dispositifs et des protocoles de protection à partir du poste de travail, fusse-t-il un PC ou un smartphone…

Dans ce contexte, l'une des questions clés, c'est: » *comment arbitrer entre l'ouverture, la mobilité et le contrôle d'authentification: qui peut accéder à quoi? Cela implique un* ***système de défense en profondeur*** »

« *Chez Microsoft, nous répondons avec deux pièces maîtresses:*

1- ***Forefront ID manager*** **:** *un gestionnaire des profils d'identités et des accès privilégiés, modules prévus pour 2010, séparés de Windows Server R2 ; 2-***Direct Access***: un sous-ensemble de sécurisation au niveau du poste de travail, constitué de 3 produits*

.***Unified Access Gateway*** *(UAG) . Windows 7 . Windows Server 2008 R2*

Accompagnant la sortie de Windows 7, cette offre de sécurisation sera disponible d'ici à la fin 2009.