SAN et sécurité. (Paru dans LuxBox Magazine Avril 2004)

Statistiquement la plupart des sociétés investissent plus d'argent dans la sécurisation de leur site Web contenant des données statiques que dans la protection de leur SAN contenant des données vitales.

La technologie Fiber Channel et l'apparition du protocole IP dans les réseaux de stockage offrent des vulnérabilités comparables à celles du monde des réseaux d'entreprises et de l'Internet. Ce problème est encore accentué par l'utilisation de solutions d'administration de systèmes basées sur ce même protocole IP.

Les réseaux de stockage, même si ils sont rarement implantés dans ce but, peuvent être considérés comme une amélioration de la sécurité des données car ils engendrent une centralisation de l'accès aux données. A contrario la majorité de ces réseaux fournissent des données aux différents systèmes informatiques, créant parfois des ponts entre les zones DMZ, Intranet, Internet,…

Les fonctions SAN dites de sécurité, telles que le « Zoning » et le « LUN Masking » n'ont pas été conçues dans un but sécuritaire et l'implémentation basique ordinairement réalisée ne peut être considérée comme fiable.

La sécurité des SAN/NAS reste un sujet bizarrement flou. Ce qui existe dans ce domaine, notamment quelques produits dédiés et un décret de l'IETF faisant office de standard, continue d'évoluer. Ce décret concerne les équipements de stockage IP et les composants réseaux liés. Il définit que tout produit de stockage, adaptateur de bus, appareil ou logiciel de contrôle devra à l'avenir offrir des services d'authentification et cryptage basés sur IPSec. Le risque est grand que la combinaison de solutions plus ou moins propriétaires n'entraîne quelques soucis au niveau des administrateurs de stockage et que ces ajustements n'aient un impact négatif sur la stabilité d'un élément vital tel que le réseau de stockage. La nécessite de supporter des mécanismes de cryptage « à vitesse filaire » pourrait également s'avérer une gageure technologique.

Le portage des technologies de réseaux virtuels (VLAN) sur le SAN (VSAN) ainsi que la technologie d'authentification par certificats sont autant de signes d'une prise de conscience des acteurs de ce marché. Ces derniers semblent reconnaître la nécessité de résoudre la question de sécurité s'ils espèrent voir les projets de centralisation continuer à se développer.

Un plan d'intégration des réseaux de stockage dans la politique générale de sécurité devrait pour bien faire couvrir les environnements physiques et logiques du SAN mais aussi dresser une liste des risques et impacts potentiels. Sur cette base il sera dès lors possible d'établir une liste de recommandations ainsi qu'un plan d'implémentation.

Que votre choix se porte vers une solution de sécurité SAN autonome ou que vous penchiez pour une intégration dans la politique globale de sécurité, il faut être conscient que cela reste complexe et exige une savante combinaison de connaissances dans les domaines de la sécurité, du stockage et des protocoles.

DELBRASSINE Charles – IT WORKS SA