

La Fuite Des Données peut vous détruire en Bourse

Les fuites des données à la « Wikileaks » peuvent vous détruire en Bourse et ce malgré les efforts et les investissements considérables que les entreprises déploient pour sécuriser leurs informations critiques. Le défi est d'adresser les trois axes essentiels à la sécurisation de l'information soit : L'aspect humain, l'aspect processus et finalement l'aspect technologie. Cet article décrit comment la technologie a elle seule ne peut venir à bout des défis CyberÉconomiques.

Alain Scherrer, Président

La fuite de données, une menace permanente en entreprise

Le monde entier a récemment fait la connaissance du site « Wikileaks », un site web qui se spécialise dans la publication de données que d'autres voudraient taire. Cette fois, ce sont des données gouvernementales qui ont été révélées. Si un tel incident rappelle à tous le besoin de protéger ses données, il ne faut jamais oublier les règles de base au moment de concevoir sa solution de sécurité.

La première règle est trop souvent oubliée immédiatement après avoir été énoncée : la menace principale n'est pas une vulnérabilité ou une faille technologique mais bien une ressource humaine à l'intérieur à l'environnement. Les événements de Wikileaks ne sont qu'une preuve supplémentaire de ce fait. Pourtant, malgré cela, de très nombreux environnements TI ne bénéficient que d'une protection périphérique. Une telle approche n'offre aucune protection contre cette menace principale à l'interne. De plus, si un environnement est difficile à pénétrer de l'intérieur, il est automatiquement protégé aussi contre l'extérieur. Au contraire, sa protection face à l'extérieur n'est d'aucun secours contre une menace interne.

La seconde règle est connue et les gens cherchent à l'appliquer. Toutefois, ayant oublié la première règle, cette règle-ci est généralement mal appliquée : la sécurité a la force de son maillon le plus faible. Cette réalité est bien connue et acceptée, mais peu reconnaissent que le maillon faible est une ressource humaine à l'interne. Plusieurs cherchent plutôt au niveau des technologies. Le résultat est que l'on tente de renforcer les technologies pour palier aux maillons faibles.

Au début, les pare-feux devaient régler tous les problèmes de sécurité. Ce sont ensuite les serveurs proxys qui ont fait cette promesse. Le miracle ne s'étant pas produit, les sondes de détection d'intrusion (IDS) et leur sœur, celle de prévention des intrusions (IPS), sont apparues. Après un nouvel échec, la prochaine solution miracle a été les services de contrôle d'accès au réseau (NAC). Aujourd'hui, les solutions de prévention de vol de données (data loss prevention ou DLP) deviennent la nouvelle mode. Malgré que ces technologies aient grandement contribuées à sécuriser l'accès à vos données, leur échec est inévitable pour plusieurs raisons. D'une part, d'un point de vue technologique, la fonction recherchée est impossible à accomplir. Il suffit de penser à l'industrie des films et des jeux qui tente de rendre ses produits non copiables depuis toujours, en vain. D'autre part, ce produit demeure une technologie. Tel que le dicte la première règle, les ressources humaines, non les technologies, sont le maillon la plus faible.

Pour éviter des fuites de données et des incidents à la Wikileaks, une bonne gestion et sensibilisation des ressources humaines est incontournable. Les technologies aident à atteindre les objectifs fixés et sont essentielles dans l'application d'une bonne sécurité. Cependant, il ne faut pas croire qu'elles peuvent tout faire, jusqu'à remplacer les ressources humaines et leur éthique de travail.