Telindus : Armer les PME contre les cyber-criminels
Internet
Posté par : JPilo
Publiée le : 12/11/2012 13:30:00

Avec l'ouverture du système d'information des entreprises, le nombre potentiel d'attaques provenant d'Internet ne cesse d'augmenter et, pour y faire face les entreprises ne sont pas toutes correctement préparées, techniquement et organisationnelement.

Trop d'entreprises ne sont dotées que d'une protection passive, qui leur permet difficilement de réagir en cas d'attaques mais elles doivent aujourd'hui évoluer vers une protection proactive pour créer toujours plus d'obstacles sur la route des cyber-criminels, et surtout réagir rapidement pour éviter que les attaques subies ne prennent de l'ampleur.

« *Les menaces qui pèsent sur les systèmes d'information des entreprises sont une réalité, et les attaques qui ont fait les gros titres ces dernières années le montrent, les solutions de sécurité traditionnelles ne sont pas suffisantes pour se prémunir des attaques ciblées.* » explique **Noël Chazotte,** Marketing et Innovation Sécurité, Telindus France.

L'intégration seule de solutions technologiques ne sera efficace que si elles sont mises en place dans le cadre d'une stratégie dédiée. Pour accompagner les entreprises à faire face à la cyber-criminalité, Telindus, spécialiste en sécurité, a mis au point une méthodologie destinée à couvrir toutes les étapes, à prendre en compte pour s'armer au mieux contre ces nouvelles menaces. Cette approche s'appuie sur le principe de défense en profondeur que

l'on doit établir pour protéger une donnée sensible.

Elle s'articule autour de trois piliers :

- surveiller les différentes couches du SI (Infrastructure, application, données) ;

- détecter les signaux faibles des attaques parmi la multitude d'événements normaux ou anormaux ;

- réagir en prenant en compte toutes les informations possibles liées à l'événement et mettre en place la procédure liant le traitement technique et organisationnel de l'événement.

Plus concrètement, la méthode « SDR » s'appuie sur les éléments clés suivants :

- une analyse de risques basée sur les besoins métiers fonctionnels qui permet de déterminer les impacts redoutés par les métiers. Ces impacts ne sont pas forcément liés aux incidents informatiques ;

- la construction d'un indice de sécurité SDR pour chaque déclinaison fonctionnelle des besoins métiers ;

- ces indicateurs conduisent à l'établissement de tableaux de bord sur le niveau de service fourni au métier, mais également sur la manière de corriger un incident métier suite à un impact redouté.

Cette méthodologie s'inscrit dans le cadre d'une offre mise au point par Telindus et destinée à accompagner les entreprises à se prémunir contre les malveillances venant d'Internet.

Dans le cadre de cette nouvelle offre, Telindus se donne pour mission de :

- conseiller, avec un accompagnement stratégique afin de déterminer les impacts redoutés en cas d'attaques, d'analyser les risques et la mise en place de la méthode « SDR » au processus de sécurité ;

- intégrer les solutions techniques et de services (Gouvernance de données, détection des intrusions de malwares, protection contre les fuites de données sensibles, visibilités complète des échanges sur tout ou partie du SI, recherche forensic via le Security Research Center de Telindus France) ;

- gérer pour garantir un cercle d'amélioration continue (Maintenir et optimiser la qualité des processus sécurité en exploitant la méthode SDR, maintenir en conditions opérationnelles les technologies les plus sensibles, services de gestion en temps réel pour assurer une meilleure réactivité).

Pour **Nicolas Leseur**, Marketing et Innovation Sécurité, **Telindus France** : « *Même si les nouvelles solutions donnent les moyens d'agir face aux nouvelles menaces, les technologies ne sont que des outils au service d'une nouvelle approche de la sécurité qui doit être créée au sein de l'entreprise.* »