

Xavier Tardif, DG de Deny All: 'le reverse-proxy devient un standard'

Deny All est l'un des leaders européen dans le domaine de la protection des applications en ligne. Son produit phare « rWeb », basé sur une architecture 'reverse-proxy' permet d'inspecter en amont les flux http et https qui atteignent un serveur Web sur lequel une application en ligne est installée. Santy met en exergue les problèmes liés aux applicatifs Web, cas isolé ou nouvelle menace ? Les vers vont-ils de plus en plus exploiter les failles dans Php, Asp etc. ? Le nombre de vulnérabilités va de paire avec la complexité grandissante des applicatifs web. Il est clair que de plus en plus de failles vont être découvertes au coeur des applications en ligne. Santy est un bel exemple des risques liés à l'insécurité de certains scripts php mais le code du ver reste très artisanal. Malheureusement, il faut nous rendre à l'évidence, 2005 devrait nous apporter d'autres versions ou d'autres vers du même type mais plus évolués et donc plus virulents. Il y a 8 ans, Deny All avait déjà identifié ces risques. C'est ce phénomène qui est à l'origine de la création de la société. Comment se protéger efficacement contre ce genre d'attaques ? La mise en place d'une solution « reverse-proxy » en complément de l'infrastructure existante est aujourd'hui la meilleure option. Le « reverse-proxy » est devenu une brique sécurité extrêmement importante voir fondamentale. C'est la seule solution qui permet de dresser une barrière devant les requêtes et les flux http(s) agressifs. De plus il intègre généralement des fonctionnalités d'accélération et de SSO (Single Sign On). Une protection de type « reverse-proxy » permet notamment de maîtriser la sécurité dans le temps et d'adopter une démarche proactive. L'objectif est de pérenniser la sécurité. Un effet de bord remarquable, remonté par nos clients, nous montre que le « reverse proxy » peut dans certains cas apporter une visibilité supplémentaire sur le fonctionnement de l'applicatif à sécuriser. Cela facilite grandement le travail des développeurs et contribue à améliorer la sécurité globale du système d'information. Qu'est ce qui caractérise une bonne solution « reverse-proxy » ? Beaucoup de facteurs rentrent en compte. Les plus importants sont la robustesse et l'expérience de la solution. Sa capacité à s'adapter aux applicatifs du client et surtout la facilité de mise en place des règles et des protections. En quoi résident les modifications apportées à la nouvelle version de rWeb ? Nous avons beaucoup travaillé sur l'automatisation de la mise en place de règles de sécurité au sein de rWeb. Notre volonté est de simplifier au maximum l'administration du boîtier. Ainsi nous avons développé des outils de génération et de validation automatique de règles de sécurité même quand l'applicatif à protéger évolue. rWeb s'adapte, on retombe sur la « capacité d'adaptabilité » dont je parlais tout à l'heure. Nous avons également intégré la supervision SNMP et le Load Balancing dans cette nouvelle version. Quelle est la stratégie de Deny All pour l'année 2005 ? En 2004 nous avons construit un réseau de revendeurs européen en s'appuyant sur nos bureaux en Angleterre, en Espagne et au Danemark (UK, ES, DK). En 2005, nous allons continuer notre développement européen, augmenter notre présence et gagner de nouvelles références. Nous avons réussi notre objectif de 2004 qui était d'atteindre une dimension européenne. En 2005, nous allons transformer l'essai. Comment se porte le marché de la protection des applicatifs Web ? Le marché a réellement mûri en France et en Europe. Les entreprises ont pris conscience des problématiques liées à la sécurisation d'applications en ligne. Le « reverse-proxy » est en train de devenir une brique sécurité standard dans les architectures évoluées. Nous sommes en France des précurseurs dans ce domaine et le fait qu'une concurrence se mette en place nous rassure. (*)pour

